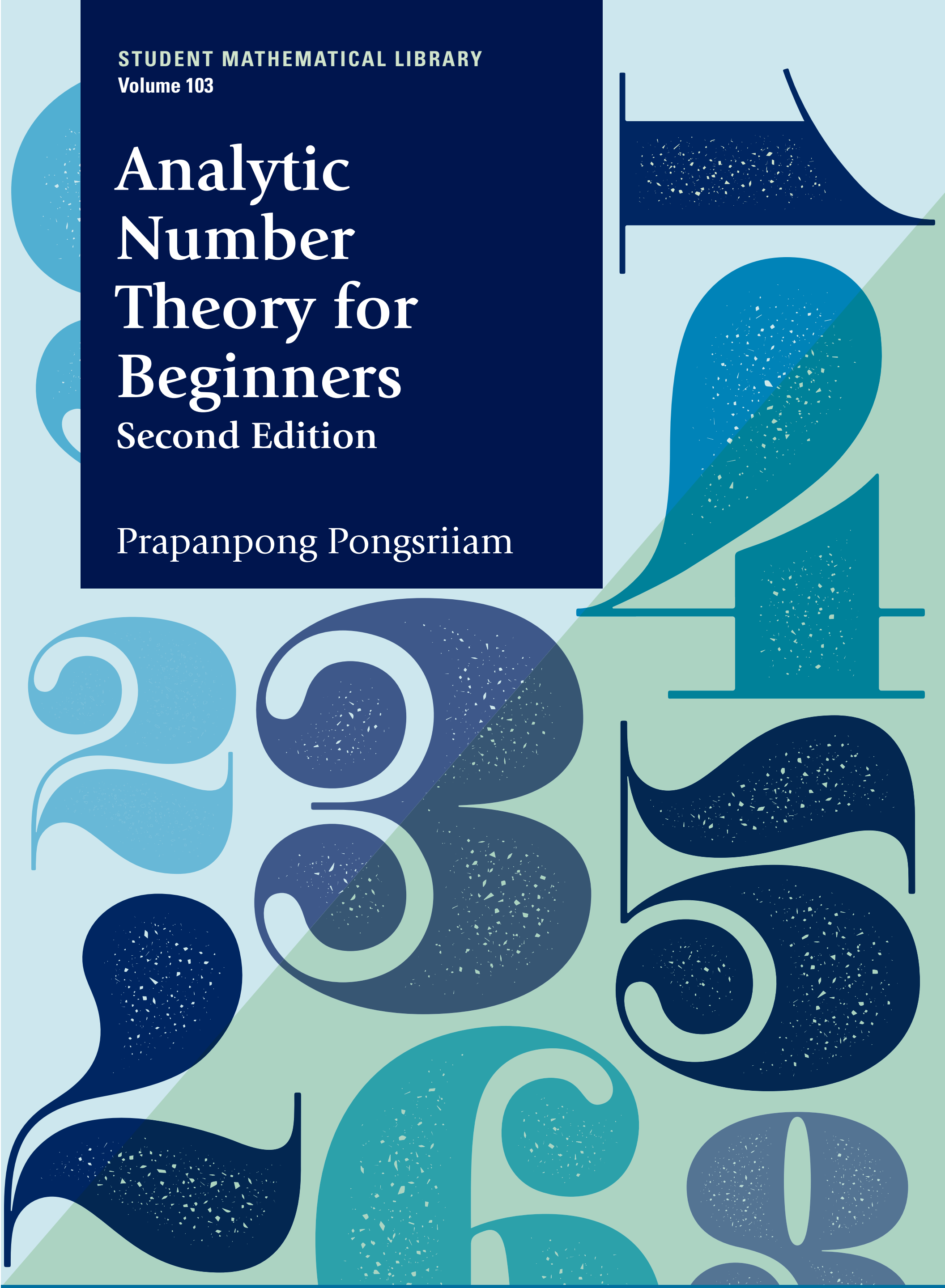
STUDENT MATHEMATICAL LIBRARY
Volume 103

# Analytic Number Theory for Beginners

## Second Edition

Prapanpong Pongsriiam



AMS
American
Mathematical
Society

# Analytic Number Theory for Beginners

## Second Edition

STUDENT MATHEMATICAL LIBRARY
Volume 103

# Analytic Number Theory for Beginners

## Second Edition

AMERICAN
MATHEMATICAL
SOCIETY
Providence, Rhode Island

## EDITORIAL COMMITTEE

John McCleary
Rosa C. Orellana (Chair)
Paul Pollack
Kavita Ramanan

2020 *Mathematics Subject Classification.* Primary 11-01, 11-02, 11Axx, 11Bxx, 11Nxx, 11Pxx.

The first edition of this book, *Introduction to Analytic Number Theory*, was published by Silpakorn University Printinghouse in Nakhon Pathom, 2020; ©2020 Prapanpong Pongsriiam, and is available only in Thailand.

For additional information and updates on this book, visit
**www.ams.org/bookpages/stml-103**

**Copying and reprinting.** Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy select pages for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for permission to reuse portions of AMS publication content are handled by the Copyright Clearance Center. For more information, please visit `www.ams.org/publications/pubpermissions`.

Send requests for translation rights and licensed reprints to `reprint-permission@ams.org`.

© 2023 by the American Mathematical Society. All rights reserved.
The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at `https://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 28 27 26 25 24 23

*Continued on page 376*

Dedicated to my best friend
Tammatada Khemaratchatakumthorn

# Contents

Preface to the Second Edition and Acknowledgment xi

Preface to the First Edition xiii

Acknowledgments xvii

Notation xix

Chapter 1. Review of Elementary Number Theory 1

§1.1. Divisibility 1
§1.2. Greatest Common Divisor 2
§1.3. Least Common Multiple 6
§1.4. Prime Numbers 6
§1.5. Congruences 10
§1.6. Residue Systems 12
§1.7. Chinese Remainder Theorem 13
§1.8. Polynomial and Some Special Congruences 17
§1.9. Lifting the Exponents 20
§1.10. Primitive Roots 22
§1.11. Quadratic Residues 23
§1.12. Sum of Squares 24
§1.13. Exercises 25

§1.14. Notes 26

Chapter 2. Arithmetic Functions I 33
§2.1. Introduction 33
§2.2. Multiplicative Functions 36
§2.3. Dirichlet Product 38
§2.4. Divisor Sums and the Möbius Inversion Formula 42
§2.5. Extensions of the Möbius Inversion Formula 49
§2.6. Exercises 52
§2.7. Notes 56

Chapter 3. The Floor Function 65
§3.1. Introduction 65
§3.2. Hermite's Identity and Generalizations 71
§3.3. Counting Lattice Points 79
§3.4. Miscellaneous Examples 85
§3.5. Exercises 90
§3.6. Notes 93

Chapter 4. Summation Formulas 99
§4.1. Introduction 99
§4.2. Big $O$, Little $o$, and Related Notations 100
§4.3. Sums of Monotone Functions 104
§4.4. Partial Summation Formula 108
§4.5. Review of the Riemann-Stieltjes Integral 112
§4.6. Euler Summation Formula 114
§4.7. Euler-Maclaurin Summation Formula 117
§4.8. Exercises 121
§4.9. Notes 123

Chapter 5. Arithmetic Functions II 129
§5.1. Introduction 129
§5.2. Average Orders 131
§5.3. Dirichlet's Hyperbola Method 137

§5.4. Extremal Orders 141
§5.5. Normal Orders 150
§5.6. Exercises 154
§5.7. Notes 161

Chapter 6. Elementary Results on the Distribution of Primes 169
§6.1. Introduction 169
§6.2. Chebyshev's Estimates 173
§6.3. Mertens' Theorems 178
§6.4. Exercises 181
§6.5. Notes 184

Chapter 7. Characters and Dirichlet's Theorem 187
§7.1. Introduction 187
§7.2. The Orthogonality Relations 192
§7.3. Dirichlet Characters 194
§7.4. Dirichlet $L$-Functions 198
§7.5. Dirichlet's Theorem 202
§7.6. Applications of Dirichlet's Theorem 208
§7.7. The Statement of the Green-Tao Theorem 214
§7.8. Exercises 215
§7.9. Notes 221

Chapter 8. The Riemann Zeta Function 229
§8.1. Introduction 229
§8.2. Half-Plane of Convergence 231
§8.3. Review of Infinite Products 238
§8.4. Euler Product Formula 242
§8.5. Analytic Continuation 247
§8.6. Zero Free Regions 249
§8.7. Exercises 251
§8.8. Notes 253

Chapter 9. Prime Number Theorem and Some Extensions 257

§9.1. Introduction 257
§9.2. Proof of the Prime Number Theorem 259
§9.3. Elementary Proof of the Prime Number Theorem 264
§9.4. Stronger Forms of the Prime Number Theorem 267
§9.5. Integers Having $k$ Prime Factors 269
§9.6. Exercises 280
§9.7. Notes on Prime in Arithmetic Progressions 285
§9.8. Analogues of the Bombieri-Vinogradov Theorem 288
§9.9. Notes on Bounded Gaps Between Primes 290

Chapter 10. Introduction to Other Topics 293
§10.1. Idea of Sieves 293
§10.2. Brun's Sieve 295
§10.3. Selberg's Sieve 303
§10.4. Introduction to Additive Number Theory 313
§10.5. Schnirelmann's Basis Theorem 321
§10.6. An Outline of the Circle Method in Waring's Problem 329

Chapter 11. Hints for Selected Exercises 335
Hints for Exercises 1.13 335
Hints for Exercises 2.6 336
Hints for Exercises 3.5 337
Hints for Exercises 4.8 339
Hints for Exercises 5.6 340
Hints for Exercises 6.4 342
Hints for Exercises 7.8 344
Hints for Exercises 8.7 346

Bibliography 347

Subject Index 367

Name Index 371

# Preface to the Second Edition and Acknowledgment

Chapter 10 on an introduction to sieve methods and additive number theory is added. I originally intended to separate these two topics, but for simplicity, I combined them into a single chapter. This is a new chapter that does not appear in the first edition.

Some typographical and grammatical errors are corrected. The notes at the end of each chapter are updated. English and latex sentences are slightly changed to remove some bad boxes, which occur due to the change of latex style from the first to the second edition. Although I tried to remove as many of them as possible, some bad boxes are left unchanged. I apologize for any inconvenience.

I hope the reader enjoys reading this book, and if you have any comments or suggestions, please send me an email at `prapanpong@gmail.com` or `pongsriiam_p@silpakorn.edu`. I will also put the list of updates on my google homepage at `https://sites.google.com/view/math-prapanpong-pongsriiam/teaching`.

Many people have supported me, directly or indirectly, during the preparation of this book. Some of their names already appeared in the first edition, but there are others I would like to mention too.

First of all, I would like to thank the editors Eriko Hironaka and Ina Mette for their patience and understanding during the revision and publication process. The reviewers gave me an insight and made me aware of some references that I could use to update my notes. They also suggested that I write a new chapter on sieve methods and additive number theory, and recommended that I add more prose and connecting sentences. I thanks all three anonymous reviewers for their kind comments and useful suggestions which improved the quality of the manuscript. I will be glad if this book meets parts of their expectations.

Associate Professor Wanida Hemakul supported me in the application of the Tosio Kato Fellowship of the Mathematical Society of Japan. Professor Kohji Matsumoto agreed to be my host professor and let me do research at Nagoya University. The draft of the second edition was first written while I was working in Thailand, but the final version was finished when I visited Nagoya University in Japan. The Library of Nagoya University let me have access to several books, articles, references, and the important database MathScinet™, which I did not have access to while I was in Thailand. Yuko Ikuta and her colleagues helped me with some of the paper work. I am thankful to all of them.

Most importantly, I am very grateful to Tammatada Khemaratchatakumthorn for helping me prepare the entire draft of both the first and second editions.

Prapanpong Pongsriiam

Silpakorn University, Nakhon Pathom (Thailand) and

Nagoya University, Nagoya (Japan)

November 2022

# Preface to the First Edition

I took several mathematics courses when I was a graduate student at Penn State University. With Professor Vaughan's teaching and the book by Professors Montgomery and Vaughan as references, I decided to write a lecture note on analytic number theory which was accessible to beginners.

My small lecture note has gradually been expanded from various courses, seminars, and conference talks I have given at Silpakorn University and many other institutions. It has been distributed among the audiences ranging from advanced high school to doctoral students, and it has finally become this text. While most textbooks on the same subject are written for advanced graduate students or researchers, this book contains the material for both undergraduate and graduate students, and also offers a transition between them.

Chapters 1 to 3 have been used in undergraduate teaching and also in the training of selected students at IPST for International Mathematical Olympiad. Chapters 4 to 9 are for graduate students and any reader who would like a taste of analytic number theory. The prerequisites for this book are undergraduate courses in elementary number theory, real analysis, complex analysis, and abstract algebra. Beyond this, the volume is self-contained. I show the details of the proofs as much as possible so that the readers can follow them easily. However, some parts may be more difficult than the others, and therefore it is optional to study or skip them in the first reading. This option is clearly indicated in the second part given below.

Examples and exercises are of varying difficulty and are collected from classic texts, mathematical competitions, and my personal notes taken when I attended Professor Vaughan's lecture; some are from my design; some are from joint work with my students; many of these are connected with possible research projects for students and researchers. I have also tried to give credit to the sources of each exercise. However, I may miss something. If the readers find anything inaccurate, I will be happy to learn more and will adjust my book accordingly.

At the end of each chapter, I intentionally record many things in the notes including a summary of the lessons, a source and a connection of exercises with open questions, a short history of an invention in mathematics, an entertaining fact, my results that are related to the chapter, and my thoughts on some open problems. Unlike many other books on the same subject, I point to various directions in the hope that the readers may get new ideas not only on the central topic but also totally different topics of research. I think this gives a broadly accessible survey and a wider view of analytic-combinatorial-elementary number theory, and I hope this provides the interested reader with ample material to pursue.

It will be a pleasure too if the readers solve some of my proposed problems or any other related research question, get them published, and let me know the answer. Please send any comments to my email at `prapanpong@gmail.com` or `pongsriiam_p@silpakorn.edu`. I will also post a list of errata and other updates on my homepage in the future.

**How to Use This Book.** Chapter 1 (except the notes) is just a review of elementary number theory. So the reader may read through it quickly. Chapter 2 is also known to undergraduate students, but our presentation is quite different, and studying it will help the reader get familiar with the basic calculations in later chapters. Chapter 3 on the floor function is interesting on its own and can be used as a supplementary reading for undergraduates, but reading only Definition 3.1 and Theorem 3.3 is more than enough for understanding the other chapters. Chapter 4 gives the basic notation and summation formulas that are used throughout this text. Chapters 5 to 9 contain the main material for the first course in analytic number theory. However, Sections 4.7, 5.4, 5.5, and 9.3 to 9.9 may be skipped in the first reading.

It is not necessary to solve all the exercises. Although many theorems in number theory are very difficult to prove, understanding their statements is easy. So whenever we refer to a result in an exercise, the readers can simply assume that it is true, use it in any way they like, and then come back at a time later to solve it. In fact, exercises are often cited in the notes but only one theorem (Theorem 5.7) depends on an exercise.

Notes at the end of each chapter are meant to entertain and inform the readers on old and new results in mathematics; they are not used in the proofs of any theorems in this book, and so the readers do not have to study all of them. Although the notes may depend heavily on my preferences, they contain the discussion of research that is related to the main material and exercises. Some research problems may be suitable for students and I hope that experts and instructors can also use these in their teaching. Perhaps my favorite topics are in the notes of Chapters 1, 2, 3, 4, 5, 7 and 9. I hope the readers will like them too. Again, I welcome any suggestions from the readers.

Prapanpong Pongsriiam

Silpakorn University
Nakhon Pathom
March 2020

# Acknowledgments

Many thanks to Professor Robert Vaughan for teaching me the beautiful subject of number theory, for always supporting me in doing anything in mathematics, and for being a great inspiration. His lecture influences the content and the writing style of this book. Thanks also go to other teachers, especially Associate Professor Ajchara Harnchoowong, Professor Wen-Ching Winnie Li, Professor Bruce Berndt, Professor Bruce Reznick, and Professor Ram Murty, for giving me an opportunity to learn from them.

Silpakorn and Penn State Libraries, and Teeradej Kittipassorn provided me with data support. Teerapat Srichan, Saran Intapiu, Kantaphon Kuhapatanakul, Donny Passary, Thotsaporn Thanatipanonda, and Elaine Wong sent me some documents which enabled me to update my book conveniently.

Friends, students, supporters, and followers directly or indirectly encouraged me to do this work. They are Lida Ing, Kosin Panyaatisin, Paveena Srirangsan, Patcharee Sumritnorrapong, Youngwoo Kwon, Uthumporn Domthong, Supawadee Prugsapitak, Narissara Khaochim, Phakhinkon Phunphayap, Kritkhajohn Onphaeng, Chalinee Khaochim, Saralee Aursukaree, Sutasinee Kawsumarng, Blazej Zmija, Kittipong Subwattanachai, Niphawan Phoopha, Sawian Jaidee, Montree Jaidee, Passawan Noppakaew, and Asim Patra. In particular, by running the computation on his computer, Phakhinkon Phunphayap has assisted me

in collecting numerical data for my research, which in turn supported me in designing some exercises and expanding some notes.

The Faculty of Science at Silpakorn University has given me financial support[1] and had my manuscript reviewed by three external reviewers whose comments and suggestions helped to improve the quality of this book.

The editors and reviewers of the American Mathematical Society (AMS) also reviewed my manuscript and gave recommendations. I would like to thank them for their generosity for allowing me to distribute the first edition of the book before adding two or three more chapters and publishing the new version with the AMS as this second edition. By the way, the topics to be added are on sieve methods, additive number theory, and the circle method.

I have several opportunities to join and give talks in the seminars organized by Aram Tangboonduangjit, Thotsaporn Thanatipanonda, Chatchawan Panraksa, and Pornrat Ruengrot at Mahidol University International College (MUIC). Their hospitality and the academic atmosphere at MUIC remind me of the good old days when I was listening to Professor Vaughan's lectures and attending seminars at Penn State and other institutions. In addition, I thank Professor Vichian Laohakosol and his students for organizing the CNA and ICNA conferences every year, which promotes the research activity among my students and other number theorists in Thailand.

Special thanks go to Nobuo Uematsu, Yasunori Mitsuda, Kenji Ito, Yoko Shimomura, Hiroki Kikuta, and other musicians and artists at Square Soft (now Square Enix) for making the video games enjoyable and beautiful. Listening to their music not only brings back the exciting adventures and good memories of my childhood but also gives me a lot of energy to work on mathematics.

Last but not least, I am very grateful to Tammatada Khemaratchatakumthorn who helped me prepare the entire manuscript and has been supporting me in all other aspects of my life. Without her, this text would never have appeared. Any good coming from this is dedicated to her.

Prapanpong Pongsriiam

---

[1] The first edition of this book was written under Silpakorn Book Project and was supported by the Faculty of Science, Silpakorn University, grant number SRIF–TBG–2562–07.

# Notation

| | |
|---|---|
| $a \mid b$ | $a$ divides $b$, $b$ is divisible by $a$ |
| $a \nmid b$ | $a$ does not divide $b$, $b$ is not divisible by $a$ |
| $a^k \parallel b$ | $a^k \mid b$ and $a^{k+1} \nmid b$ |
| $\mathbb{Z}$ | the set of all integers |
| $\mathbb{Z}^+$, $\mathbb{N}$ | the set of all positive integers, the set of all natural numbers |
| $\mathbb{Q}$ | the set of all rational numbers |
| $\mathbb{R}$ | the set of all real numbers |
| $\mathbb{C}$ | the set of all complex numbers |
| $A - B, A \setminus B$ | the set of all elements of $A$ that are not in $B$ |
| $\#A$, $\lvert A\rvert$ | the number of the elements in the set $A$, the cardinality of the set $A$ |
| $\gcd(a, b)$ | the greatest common divisor of $a$ and $b$ |
| $(a, b)$ | the greatest common divisor of $a$ and $b$ or the point $(a, b)$ in a plane or the open interval $(a, b)$ (depending on the context) |
| $\gcd(a_1, a_2, \ldots, a_n)$ | the greatest common divisor of $a_1, a_2, \ldots, a_n$ |
| $(a_1, a_2, \ldots, a_n)$ | the greatest common divisor of $a_1, a_2, \ldots, a_n$ or the point $(a_1, a_2, \ldots, a_n)$ in $\mathbb{R}^n$ |
| $\gcd(A)$ | the greatest common divisor of the elements of the set $A$ |
| $\operatorname{lcm}[a, b]$ | the least common multiple of $a$ and $b$ |

| | |
|---|---|
| $[a, b]$ | the least common multiple of $a$ and $b$ or the closed interval (depending on the context) |
| $[a_1, a_2, \dots, a_n]$ or $\operatorname{lcm}[a_1, a_2, \dots, a_n]$ | the least common multiple of $a_1, a_2, \dots, a_n$ |
| $v_p(n)$ | the $p$-adic valuation of $n$, the $p$-adic order of $n$, the exponent of $p$ in the prime factorization of $n$ |
| $a \equiv b \pmod{m}$ | $m \mid a - b$ |
| $a \not\equiv b \pmod{m}$ | $m \nmid a - b$ |
| $a \bmod m$ | the remainder in the division of $a$ by $m$, the least nonnegative residue of $a$ modulo $m$ |
| $\mathbb{Z}[x]$ | the set of polynomials in $x$ with integer coefficients |
| $\varphi(n)$ | Euler's function of $n$, the number of integers $k$ such that $1 \le k \le n$ and $(k, n) = 1$ |
| $n!$ | factorial of $n$, the product $1 \cdot 2 \cdot 3 \cdots n$ |
| $\operatorname{ord}_m a$ | the order of $a$ modulo $m$, the smallest positive integer $k$ such that $a^k \equiv 1 \pmod{m}$ |
| $\left(\frac{a}{p}\right)$ | Legendre symbol |
| $s(n)$ | the sum of digits of $n$ in the decimal representation of $n$ |
| $s_b(n)$ | the sum of digits of $n$ when $n$ is written in base $b$ |
| $F_n$ | the $n$th Fibonacci number |
| $d(n)$, $\tau(n)$ | the number of positive divisors of $n$ |
| $\sigma(n)$ | the sum of positive divisors of $n$ |
| $\sigma_\alpha(n)$ | the sum of $d^\alpha$ where $d$ ranges over the positive divisors of $n$ |
| $1(n)$ | is equal to 1 for every $n \in \mathbb{N}$ |
| $N(n)$ | is equal to $n$ for every $n \in \mathbb{N}$ |
| $e(n)$ | is equal to 1 if $n = 1$ and 0 otherwise |
| $\omega(n)$ | the number of distinct prime divisors of $n$ |
| $\Omega(n)$ | the number of prime divisors of $n$ counted with multiplicity |
| $\mu(n)$ | is equal to $(-1)^{\omega(n)}$ if $n$ is squarefree and 0 otherwise |

| | |
|---|---|
| $\lambda(n)$ | is equal to $(-1)^{\Omega(n)}$ |
| $\Lambda(n)$ | is equal to $\log p$ if $n = p^k$ for some prime $p$ and a positive integer $k$; otherwise it is 0 |
| $\mathcal{A}$ | the set of all arithmetic functions |
| $\mathcal{A}^{\times}$ | the set of all arithmetic functions $f$ such that $f(1) \neq 0$ |
| $\mathcal{M}$ | the set of all multiplicative functions |
| $\sum\limits_{d \mid n} f(d)$ | the sum of $f(d)$ where $d$ ranges over the positive divisors of $n$ |
| $(f * g)(n)$ | $\sum\limits_{d \mid n} f(d) g\left(\frac{n}{d}\right)$ |
| $\gamma(n)$ | $\prod\limits_{p \mid n} p$, the largest squarefree divisor of $n$ |
| $\binom{n}{k}$ | the binomial coefficient, $\frac{n!}{k!(n-k)!}$ if $n \geq k \geq 0$, and 0 if $n \geq 0$ but $k < 0$ or $k > n$ |
| $\log x$ | the natural logarithm of $x$ |
| $\lfloor x \rfloor$ | the largest integer that is less than or equal to $x$, the floor of $x$, the integer part of $x$ |
| $\lceil x \rceil$ | the smallest integer that is larger than or equal to $x$, the ceiling of $x$ |
| $\{x\}$ | $x - \lfloor x \rfloor$, the fractional part of $x$ |
| $[P]$ | the Iverson notation of $P$ which is 1 if $P$ is true, otherwise it is zero |
| $((x))$ | $x - \lfloor x \rfloor - 1/2$, the saw tooth function of $x$ |
| $\sum\limits_{n \leq x} f(n)$ | the sum of $f(n)$ over the positive integers $n \leq x$ |
| $\sum\limits_{y < n \leq x} f(n)$ | the sum of $f(n)$ over the positive integers $n$ in $(y, x]$ |
| $\gamma$ | Euler's constant, $1 - \int_1^{\infty} \frac{\{t\}}{t^2} dt$, $\lim_{x \to \infty} \left( \sum_{n \leq x} \frac{1}{n} - \log x \right)$ |
| $B_n(x)$ | Bernoulli polynomials |
| $B_n$ | Bernoulli numbers |
| $\pi(x)$ | the number of prime numbers that are less than or equal to $x$ |

| | |
|---|---|
| $\sum_p$ | the sum taken over primes |
| $\prod_p$ | the product taken over primes |
| $\theta(x)$ | $\sum_{p\le x}\log p$ |
| $\psi(x)$ | $\sum_{n\le x}\Lambda(n)$ |
| $p_n$ | a prime, or the $n$th prime (depending on the context) |
| $\mathbb{C}^\times$ | the set of all nonzero complex numbers |
| $G=\langle g\rangle$ | $G$ is the cyclic group generated by $g$ |
| $\chi$ | a character of $G$, a Dirichlet character |
| $\chi_0$ | the principal character |
| $e^x$, $\exp(x)$ | exponential function of $x$ |
| $e(\alpha)$ | $e^{2\pi i\alpha}$ |
| $\widehat{G}$ | the dual group of $G$ |
| $(\mathbb{Z}/q\mathbb{Z})^\times$ | the group of reduced residue classes modulo $q$ |
| $L(s,\chi)$ | $\sum_{n=1}^{\infty}\chi(n)n^{-s}$ |
| $\mathrm{li}(x)$ | the logarithmic integral $\int_2^x(1/\log t)dt$ |
| $A(a,q)$ | the set of $n\in\mathbb{N}$ such that $n\equiv a \pmod q$ or the infinite sequence $(a+qn)_{n\ge0}$ |
| $P(n)$ | the largest prime factor of $n\ge2$ and if $n=1$, then $P(n)=1$ |
| $\zeta(s)$ | $\sum_{n=1}^{\infty}n^{-s}$ |
| $\sigma_c$ | the abscissa of convergence |
| $\sigma_a$ | the abscissa of absolute convergence |
| $\sigma$, $\mathrm{Re}(s)$ | the real part of the complex number $s$ |
| $t$, $\mathrm{Im}(s)$ | the imaginary part of the complex number $s$ |
| $c_r(a)$ | Ramanujan's sum, $\sum_b e(ba/r)$ where $b$ ranges over positive integers $\le r$ that are coprime to $r$ |
| $\pi(x,q,a)$ | the number of primes $p\le x$ such that $p\equiv a \pmod q$ |
| $\theta(x,q,a)$ | $\sum_p\log p$ where $p$ ranges over primes $\le x$ such that $p\equiv a \pmod q$ |
| $\psi(x,q,a)$ | $\sum_n\Lambda(n)$ where $n$ ranges over positive integers $\le x$ such that $n\equiv a \pmod q$ |
| $\pi_k(x)$ | the number of positive integers $n\le x$ such that $\omega(n)=\Omega(n)=k$ |
| $\pi_k^{\Omega}(x)$ | the number of positive integers $n\le x$ such that $\Omega(n)=k$ |
| $\pi_k^{\omega}(x)$ | the number of positive integers $n\le x$ such that $\omega(n)=k$ |

| | |
|---|---|
| $f(x) = O(g(x))$ | there exists a constant $M > 0$ such that $\lvert f(x)\rvert \le Mg(x)$ for all $x$ in a specified domain |
| $f(x) = O^*(g(x))$ | $\lvert f(x)\rvert \le g(x)$ for all $x$ in a specified domain |
| $f(x) \ll g(x)$ | $f(x) = O(g(x))$ |
| $f(x) \gg g(x)$ | $g(x) \ll f(x)$ |
| $f(x) = o(g(x))$ | $\lim\limits_{x\to\infty} f(x)/g(x) = 0$ |
| $f(x) = g(x) + O(h(x))$ | $f(x) - g(x) = O(h(x))$ |
| $f(x) = g(x) + o(h(x))$ | $f(x) - g(x) = o(h(x))$ |
| $f(x) \asymp g(x)$ | $f(x) \ll g(x)$ and $f(x) \gg g(x)$ |
| $f(x) \sim g(x)$ | $\lim\limits_{x\to\infty} f(x)/g(x) = 1$ |

## Chapter 1

# Review of Elementary Number Theory

In this chapter, we give a summary on elementary topics which are usually taught in a first course in number theory such as divisibility properties, prime numbers, and congruences. Many theorems in this chapter are given without proof but they can be found in standard texts such as those by Apostol [**18**], Hardy and Wright [**179**], Niven, Zuckerman, and Montgomery [**290**], and Rosen [**348**]. Nevertheless, if the results may be unfamiliar to some readers or if the idea might be useful later, we either give a proof or refer them to a specific reference. Throughout this chapter, the letters $a$, $b$, $c$, $d$, $k$, $m$, $n$ denote integers.

### 1.1. Divisibility

For $a \neq 0$, we say that $a$ *divides* $b$ or $b$ is *divisible* by $a$ and we write $a \mid b$ if there exists $c$ such that $b = ac$. If $a$ does not divide $b$, we write $a \nmid b$. As usual, we exclude the division by zero. So if we write $a \mid b$, it is automatically assumed that $a$ is a nonzero integer. Other languages for the divisibility $a \mid b$ are that $a$ is a *divisor* of $b$, $a$ is a *factor* of $b$, and that $b$ is a *multiple* of $a$. In addition, if $a \mid b$ and $0 < a < b$, then $a$ is called a *proper divisor* of $b$. We also write $a^k \parallel b$ and say that $a^k$ *exactly divides* $b$ or $b$ is *exactly divisible* by $a^k$ if $a^k \mid b$ and $a^{k+1} \nmid b$. Basic properties of divisibility are as follows.

**Theorem 1.1.** *The following statements hold.*

- (i) $1 \mid a$, $a \mid 0$, *and* $a \mid a$.
- (ii) $a \mid b$ *and* $b \mid c$ *imply* $a \mid c$.
- (iii) $a \mid b$ *implies* $a \mid bx$ *for every* $x \in \mathbb{Z}$.
- (iv) $a \mid b$ *if and only if* $ac \mid bc$.
- (v) $a \mid b$ *and* $a \mid c$ *imply* $a \mid bx + cy$ *for every* $x, y \in \mathbb{Z}$.
- (vi) $a \mid b$ *and* $b \neq 0$ *imply* $|a| \leq |b|$.
- (vii) $a \mid b$ *and* $b \mid a$ *imply* $|a| = |b|$.

**Theorem 1.2.** (Division Algorithm) *Let* $a \in \mathbb{Z}$ *and* $b \in \mathbb{Z} \setminus \{0\}$. *Then there exists a unique pair of integers* $q, r$ *such that* $a = bq + r$ *and* $0 \leq r < |b|$. (*The integer* $q$ *is called the* quotient *and* $r$ *is called the* remainder.)

The reader is perhaps familiar with Theorem 1.2 but there is a different version of the division algorithm as follows.

**Theorem 1.3.** (Division Algorithm Version 2) *Suppose* $a, b \in \mathbb{R}$ *and* $b \neq 0$. *Then there exists a unique pair* $q, r$ *such that* $q \in \mathbb{Z}$ *and* $r \in \mathbb{R}$, $a = bq + r$, *and* $0 \leq r < |b|$. *In addition, if* $a, b \in \mathbb{Z}$, *then* $r \in \mathbb{Z}$.

**Proof.** For convenience, we assume that $b > 0$ (the proof is similar for $b < 0$). Since $a \in \mathbb{R} = \bigcup_{q \in \mathbb{Z}} [bq, b(q+1))$, there exists $q \in \mathbb{Z}$ such that $a \in [bq, b(q+1))$. Let $r = a - bq$. Then $a = bq + r$ and $0 \leq r < |b|$, as required. For the uniqueness, if $a = bq_1 + r_1 = bq_2 + r_2$ where $q_1, q_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < |b|$, then $|q_1 - q_2| = |r_2 - r_1|/|b| < 1$, which implies $q_1 = q_2$ and $r_1 = r_2$. The rest is obvious. ☐

## 1.2. Greatest Common Divisor

If $d \mid a$, then we say that $d$ is a divisor of $a$. If $d \mid a$ and $d \mid b$, then $d$ is called a *common divisor* of $a$ and $b$. Suppose that $a \neq 0$ or $b \neq 0$ and let $A$ be the set of common divisors of $a$ and $b$. Then $A$ is nonempty because $1 \in A$. In addition, by Theorem 1.1(vi), the set $A$ is finite. Therefore the maximum of $A$ exists and we say that $d$ is the *greatest common divisor* of $a$ and $b$ if $d = \max A$, that is, $d \mid a$, $d \mid b$, and $d \geq c$ for every common divisor $c$ of $a$ and $b$. In this case, we write $d = \gcd(a, b)$ or simply $d = (a, b)$ if no confusion arises. If $(a, b) = 1$, then we say that $a$ and $b$ are relatively prime (or $a$ and $b$ are coprime). We exclude the case $a = b = 0$ in the definition of $\gcd(a, b)$ because zero is divisible by every positive integer, and hence there is no largest common divisor of $a$ and $b$. So if we write $\gcd(a, b)$ or $(a, b)$, it is automatically assumed that $a \neq 0$ or $b \neq 0$.

*The Euclidean algorithm*, a process in which we apply the division algorithm repeatedly, can be used to find $\gcd(a, b)$ for any pair of positive integers $a, b$ and to explicitly obtain $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$. More precisely, we have the following result.

**Theorem 1.4.** (Euclidean Algorithm) *Assume that $a$, $b$ are positive integers and $q_1, q_2, \dots, q_{n-1}, r_1, r_2, \dots, r_n$ are integers satisfying the following relations:*

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b, \\ b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\vdots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} &= r_{n-1}q_n + r_n, \quad r_n = 0. \end{aligned}$$

*Then $r_{n-1}$, the last nonzero remainder in these relations, is equal to* $\gcd(a, b)$. *Furthermore, by writing the above relations backward as*

$$\begin{aligned} r_{n-1} &= r_{n-3} - r_{n-2}q_{n-1} = r_{n-3} - (r_{n-4} - r_{n-3}q_{n-2})q_{n-1} \\ &= r_{n-4}(-q_{n-1}) + r_{n-3}(1 + q_{n-2}q_{n-1}) = f_3(r_{n-3}, r_{n-4}) \\ &= f_4(r_{n-4}, r_{n-5}) = \cdots = f_{n-2}(r_2, r_1) = f_{n-1}(a, b), \end{aligned}$$

*we obtain $x, y \in \mathbb{Z}$ such that $r_{n-1} = ax + by$. Here for each $i = 3, \dots, n-2$, we write $f_i(r_{n-i}, r_{n-i-1})$ and $f_{n-1}(a, b)$ to denote linear combinations of $r_{n-i}$ and $r_{n-i-1}$ and of $a$ and $b$, respectively. In other words, if $d = (a, b)$, then there are $x, y \in \mathbb{Z}$ such that $d = ax + by$.*

**Example 1.5.** Let $a = 372$ and $b = 48$. By the Euclidean algorithm, we obtain $372 = 48(7) + 36$, $48 = 36(1) + 12$, $36 = 12(3) + 0$. In addition, we have

$$12 = 48 - 36(1) = 48 - (372 - 48(7)) = 372(-1) + 48(8).$$

Therefore $(a, b) = 12$ and we can write $12 = ax + by$ where $x = -1$ and $y = 8$. Such a pair $(x, y)$ is not unique. For instance, $12 = ax + by$ also holds when $x = 3$ and $y = -23$. In fact, there are infinitely many integers $x$, $y$ satisfying $12 = ax + by$ as shown in Theorem 1.8. Other basic properties of the greatest common divisors are given in Theorems 1.6 and 1.7.

**Theorem 1.6.** *Assume that* $a \neq 0$ *or* $b \neq 0$. *Then* $d = (a, b)$ *if and only if*

(i) $d > 0$, $d \mid a$, $d \mid b$, *and*

(ii) *if* $c \mid a$ *and* $c \mid b$, *then* $c \mid d$.

**Theorem 1.7.** *The following statements hold.*

(i) $(a, b)$ *is the smallest positive integer which can be written as* $ax + by$ *for some* $x, y \in \mathbb{Z}$.

(ii) $(a, b) = (b, a)$.

(iii) $(a, 1) = (1, a) = 1$.

(iv) $(a, b) = (-a, b) = (a, -b) = (-a, -b) = (|a|, |b|)$.

(v) $(a, b) = 1$ *if and only if there exist* $x, y \in \mathbb{Z}$ *such that*

$$1 = ax + by.$$

(vi) $d = (a, b)$ *implies* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

(vii) *If* $(a, b) = (a, c) = 1$, *then* $(a, bc) = 1$.

(viii) $(ca, cb) = |c|(a, b)$.

(ix) $a \mid b$ *implies* $(a, b) = |a|$.

(x) $(a, 0) = (0, a) = |a|$.

(xi) *If* $a \mid bc$ *and* $(a, b) = 1$, *then* $a \mid c$.

(xii) $(a + bc, b) = (a, b)$.

If $a, b, c \in \mathbb{Z}$ are given, then we can use the greatest common divisor and the Euclidean algorithm to solve the Diophantine equation $ax + by = c$ as shown in the next theorem.

**Theorem 1.8.** *Let* $a, b$, *and* $c$ *be integers and let* $d = (a, b)$. *Consider the Diophantine equation* $ax + by = c$. *If* $d \nmid c$, *then the equation has no solution in integers* $x$, $y$. *If* $d \mid c$, *then the equation has infinitely many solutions in integers. Furthermore, if* $x = x_0$, $y = y_0$ *is a solution, then all solutions are given by*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad \text{where } t \in \mathbb{Z}.$$

The concept of the greatest common divisor can be extended to more than two integers. We say that $d$ is a *common divisor of integers* $a_1, a_2, \dots, a_n$ if $d \mid a_i$ for every $i = 1, 2, \dots, n$. Suppose that at least one of $a_1, a_2, \dots, a_n$ is not zero. Then the greatest common divisor of $a_1, a_2, \dots, a_n$ is defined as the maximum of the set of all common divisors of $a_1, a_2, \dots, a_n$ and is denoted by

$$\gcd(a_1, a_2, \dots, a_n) \text{ or simply } (a_1, a_2, \dots, a_n).$$

Therefore $d = \gcd(a_1, a_2, \dots, a_n)$ if and only if $d \mid a_i$ for every $i = 1, 2, \dots, n$ and $d \geq c$ for every common divisor $c$ of $a_1, a_2, \dots, a_n$. The results for $\gcd(a_1, a_2, \dots, a_n)$ analogous to Theorems 1.6 and 1.7 are as follows.

**Theorem 1.9.** *Let* $a_1, a_2, \dots, a_n$ *be integers and let* $a_i \neq 0$ *for some* $i \in \{1, 2, \dots, n\}$. *Then* $d = \gcd(a_1, a_2, \dots, a_n)$ *if and only if*

(i) $d > 0$, $d \mid a_i$ *for every* $i$, *and*

(ii) *if* $c \mid a_i$ *for every* $i = 1, 2, \dots, n$, *then* $c \mid d$.

If $n \geq 3$ and $a_n = 0$, then $(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_{n-1})$. So we can disregard the zero when we calculate the greatest common divisor. In the next theorem, we therefore assume that all variables are nonzero.

**Theorem 1.10.** *Unless stated otherwise, the variables given below denote nonzero integers. Then the following statements hold.*

(i) $(a_1, a_2, \dots, a_n) = ((a_1, a_2), a_3, \dots, a_n) = ((a_1, a_2, \dots, a_{n-1}), a_n)$.

(ii) $(a_1, a_2, \dots, a_n) = (|a_1|, |a_2|, \dots, |a_n|)$.

(iii) *If* $b_1, b_2, \dots, b_n$ *is a permutation of* $a_1, a_2, \dots, a_n$, *then* $(a_1, a_2, \dots, a_n)$ *and* $(b_1, b_2, \dots, b_n)$ *are equal.*

(iv) $d = (a_1, a_2, \dots, a_n)$ *if and only if* $d$ *is the smallest positive integer that can be written as* $d = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ *for some* $x_1, x_2, \dots, x_n \in \mathbb{Z}$.

(v) $(ca_1, ca_2, \dots, ca_n) = |c|(a_1, a_2, \dots, a_n)$.

(vi) *If* $d = (a_1, a_2, \dots, a_n)$, *then* $\left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) = 1$.

In general, the greatest common divisor can be defined for an infinite set of integers as well. Let $A$ be a nonempty set of nonzero integers. If $d$ divides all elements $a \in A$, then $d$ is called a common divisor of $A$.

In addition, we say that $d$ is the greatest common divisor of $A$ and write $d = \gcd(A)$ if $d$ is a common divisor of $A$ and $d \geq c$ for every common divisor $c$ of $A$. As usual, the condition $d \geq c$ can also be replaced by $c \mid d$ for every common divisor $c$ of $A$. For more information, see the exercises and notes in Sections 1.13 and 1.14.

## 1.3. Least Common Multiple

If $a \mid m$, then $m$ is called a multiple of $a$. If $a \mid m$ and $b \mid m$, we say that $m$ is a *common multiple* of $a$ and $b$. Suppose that $a \neq 0$ and $b \neq 0$. Then $|ab|$ is a common multiple of $a$ and $b$. So the set $A$ of positive common multiples of $a$ and $b$ is nonempty. By the well-ordering principle, the minimum of $A$ exists. The number $m$ is called the *least common multiple* of $a$ and $b$ if $m = \min A$, that is, $m > 0$, $a \mid m$, $b \mid m$, and $m \leq c$ for every positive common multiple $c$ of $a$ and $b$. In this case, we write $m = \operatorname{lcm}[a, b]$ or simply $m = [a, b]$. As usual, we exclude the case $a = 0$ or $b = 0$ when we deal with $\operatorname{lcm}[a, b]$. So if we write $\operatorname{lcm}[a, b]$ or $[a, b]$, it is assumed that $a \neq 0$ and $b \neq 0$. We have an analogue of Theorem 1.6 for the least common multiple as follows.

**Theorem 1.11.** *Let $a \neq 0$ and $b \neq 0$. Then $m = [a, b]$ if and only if*

(i) *$m > 0$, $a \mid m$, $b \mid m$, and*

(ii) *if $a \mid c$ and $b \mid c$, then $m \mid c$.*

The results for $[a, b]$ analogous to Theorem 1.7 can be obtained by applying Theorem 1.16 (to be given in the next section). The least common multiple of $n$ nonzero integers ($n \geq 3$) can also be defined in a similar way as in the case $n = 2$. We have $m = [a_1, a_2, \ldots, a_n]$ if $m > 0$, $a_i \mid m$ for every $i$, and if $a_i \mid c$ for every $i$, then $m \leq c$. The details are left to the reader.

## 1.4. Prime Numbers

An integer $n$ is said to be *prime* if $n > 1$ and the only positive divisors of $n$ are 1 and $n$. If $n > 1$ and $n$ is not prime, then $n$ is said to be *composite*. Throughout the text, the letter $p$ with or without subscripts always denotes a prime number. We remark that in some situations, it may be desirable to include the negative integers such as $-2, -3, -5, \ldots$ as prime numbers, but for our purpose, primes are always positive.

Let $a$, $b$, and $n$ be positive integers. Some basic properties of primes are the following.

(i) If $p \nmid a$, then $(p, a) = 1$.
(ii) If $p \mid ab$, then $p \mid a$ or $p \mid b$.
(iii) For every positive integer $n > 1$, there exists a prime $p$ dividing $n$.
(iv) If $n$ is composite, then there exists $p \leq \sqrt{n}$ such that $p \mid n$. Equivalently, for $n > 1$, $n$ is prime if and only if for every prime $p \leq \sqrt{n}$, $p$ does not divide $n$.

Perhaps the following two theorems are among the most beautiful and simplest results on prime numbers.

**Theorem 1.12.** (Euclid) *There are infinitely many prime numbers.*

**Theorem 1.13.** (Fundamental Theorem of Arithmetic)
*Every integer $n > 1$ can be written uniquely as a product of prime numbers, apart from rearrangement of factors.*

**Remark 1.14.** By Theorem 1.13, we can write $n > 1$ as a product of primes not necessarily distinct. Then we can group the same prime and write $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where $p_1, p_2, \ldots, p_r$ are distinct primes and $a_1, a_2, \ldots, a_r$ are positive integers. This is called the *canonical factorization* of $n$ into prime powers.

In addition, suppose we let $p_n$ denote the $n$th prime. For instance, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$. Then we can also write $n = \prod_{i=1}^{\infty} p_i^{a_i}$ where each exponent $a_i \geq 0$. The product is a finite product because all but finite numbers of $a_i$ are zero. To summarize, the following is a typical way to represent a positive integer $n > 1$ as a product of primes or power of primes:

$n = p_1 p_2 \cdots p_k$ where $p_1, p_2, \ldots, p_k$ are prime numbers not necessary distinct.

$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where $p_1, p_2, \ldots, p_r$ are distinct prime numbers and $a_1, a_2, \ldots, a_r$ are positive integers.

$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where $p_1, p_2, \ldots, p_r$ are distinct prime numbers and $a_1, a_2, \ldots, a_r$ are nonnegative integers.

$n = \prod_{i=1}^{\infty} p_i^{a_i}$ where $p_i$ is the $i$th prime, $a_i \geq 0$ for each $i$, and all but finite numbers of $a_i$ are zero.

The fact that every positive integer larger than 1 can be factored as a product of primes enables us to obtain useful results in terms of primes. For example, the divisors, the greatest common divisor, and the least common multiple of nonzero integers are easily determined as given in the next theorem.

**Theorem 1.15.** *Let* $a = \prod_{i=1}^{\infty} p_i^{a_i}$ *and* $b = \prod_{i=1}^{\infty} p_i^{b_i}$ *be the canonical factorizations of a and b as discussed in Remark* 1.14. *Then*

(i) *The positive divisors of a are of the form* $\prod_{i=1}^{\infty} p_i^{c_i}$ *where* $0 \le c_i \le a_i$ *for every i,*

(ii) *the greatest common divisor and the least common multiple of a and b are given by*

$$(a, b) = \prod_{i=1}^{\infty} p_i^{d_i} \quad \textit{and} \quad [a, b] = \prod_{i=1}^{\infty} p_i^{m_i},$$

*where* $d_i = \min\{a_i, b_i\}$ *and* $m_i = \max\{a_i, b_i\}$ *for each i.*

Some connections of $(a, b)$ and $[a, b]$ are given in the next theorem.

**Theorem 1.16.** *Assume that a, b, and c are nonzero integers. Then the following statements hold.*

(i) $(a, b)[a, b] = |ab|$.

(ii) $[(a, b), c] = ([a, c], [b, c])$.

(iii) $([a, b], c) = [(a, c), (b, c)]$.

**Proof.** The formula (i) is well known. Since the statements (ii) and (iii) are similar, we only give a proof of (ii) as follows. We first write $a$, $b$, and $c$ in canonical forms:

$$a = \prod_{i=1}^{\infty} p_i^{a_i}, \quad b = \prod_{i=1}^{\infty} p_i^{b_i}, \quad c = \prod_{i=1}^{\infty} p_i^{c_i}.$$

By Theorem 1.15, the left and the right sides of (ii) are, respectively,

$$\prod_{i=1}^{\infty} p_i^{e_i} \text{ and } \prod_{i=1}^{\infty} p_i^{f_i}$$

where $e_i = \max\{c_i, \min\{a_i, b_i\}\}$, $f_i = \min\{\max\{a_i, c_i\}, \max\{b_i, c_i\}\}$ for every $i$. So we only need to show that $e_i = f_i$ for all $i$, which can be done by considering it case by case. If $\max\{a_i, b_i, c_i\} = c_i$, then $e_i = c_i = f_i$.

If $\max\{a_i, b_i, c_i\} = b_i$, then $e_i = \max\{c_i, a_i\} = f_i$. If $\max\{a_i, b_i, c_i\} = a_i$, then $e_i = \max\{c_i, b_i\} = f_i$. □

We can extend Theorem 1.16(i) to more than two integers as shown below. See also in Exercise 1.13.1 for another form of extension.

**Theorem 1.17.** *Let $a_1, a_2, \ldots, a_n$ be positive integers. For each $j = 1, 2, \ldots, n$, let $A_j$ be the product of the greatest common divisors of all possible collections of $j$ numbers chosen without repetitions from $a_1, a_2, \ldots, a_n$, that is,*

$$A_1 = \prod_{i=1}^{n} a_i, A_2 = \prod_{1 \le i < j \le n} (a_i, a_j), A_3 = \prod_{1 \le i < j < k \le n} (a_i, a_j, a_k), \ldots,$$

$$A_n = (a_1, a_2, \ldots, a_n).$$

*Let* $B_1 = \prod_{\substack{j=1 \\ j \text{ is odd}}}^{n} A_j$ *and* $B_2 = \prod_{\substack{j=1 \\ j \text{ is even}}}^{n} A_j$. *Then*

$$[a_1, a_2, \ldots, a_n] = B_1/B_2.$$

**Proof.** The proof follows from an idea similar to that of Theorem 1.16. We refer the reader to Vorobiev [**429**, pp. 73–74] for more details. □

Next we recall the definition of the $p$-adic valuation.

**Definition 1.18.** For each positive integer $n$ and each prime $p$, the *$p$-adic valuation* (or the *$p$-adic order*) of $n$, denoted by $v_p(n)$, is the exponent of $p$ in the canonical factorization of $n$ into power of primes.

For example, $v_p(1) = 0$ for every $p$, and if $n = 2^3 \cdot 3 \cdot 5^2$, then $v_2(n) = 3$, $v_3(n) = 1$, $v_5(n) = 2$, and $v_p(n) = 0$ for every prime $p \ge 7$. Some basic properties of the $p$-adic valuations are given below.

**Theorem 1.19.** *Let $a, b, d, m$, and $n$ be positive integers. Then the following statements hold.*

(i) $v_p(ab) = v_p(a) + v_p(b)$.

(ii) *If $a \mid b$, then* $v_p\left(\frac{b}{a}\right) = v_p(b) - v_p(a)$.

(iii) *$a \mid b$ if and only if $v_p(a) \le v_p(b)$ for every prime $p$.*

(iv) *$d = (a, b)$ if and only if $v_p(d) = \min\{v_p(a), v_p(b)\}$ for every prime $p$.*

(v) $m = [a, b]$ *if and only if* $v_p(m) = \max\{v_p(a), v_p(b)\}$ *for every prime p.*

(vi) $(a, b) = 1$ *if and only if* $v_p(a)v_p(b) = 0$ *for every prime p.*

**Proof.** Let $v_p(a) = k$ and $v_p(b) = \ell$. Then $a = p^k q_1$, $b = p^\ell q_2$, where $q_1$, $q_2$ are positive integers not divisible by $p$. Then $ab = p^{k+\ell} q_1 q_2$, which implies

$$v_p(ab) = k + \ell = v_p(a) + v_p(b).$$

The statement (ii) can be proved similarly. Next, we write $a$ and $b$ in the canonical forms as in Theorem 1.15. Then (iii), (iv), and (v) follow from Theorem 1.15. Finally, (vi) follows from (iv). $\square$

We can extend the domain of the $p$-adic valuations to nonzero rational numbers as follows. If $n$ is a negative integer, we let $v_p(n) = v_p(-n)$. If $n = a/b$ is a rational number $a \in \mathbb{Z} \setminus \{0\}$ and $b \in \mathbb{N}$, we define $v_p(n) = v_p(a) - v_p(b)$. Nevertheless, in this book, we only deal with $v_p(n)$ for $n \in \mathbb{N}$.

## 1.5. Congruences

Let $m > 0$. We say that $a$ is *congruent* to $b$ modulo $m$ and we write

$$a \equiv b \pmod{m}$$

if $m \mid a - b$. If $m \nmid a - b$, we write $a \not\equiv b \pmod{m}$. The number $m$ is called the *modulus of the congruence.* It is sometimes convenient to define the congruence for real numbers and write $x \equiv y \pmod{z}$ even when $x, y, z$ are not integers. To do this, recall that for each $x \in \mathbb{R}$, the largest integer less than or equal to $x$ is denoted by $\lfloor x \rfloor$, and if $a, b \in \mathbb{N}$, then the quotient $q$ and the remainder $r$ in the division of $a$ by $b$ is given by $q = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - bq = a - b\left\lfloor \frac{a}{b} \right\rfloor = a \bmod b$. Nevertheless, the quantity $a - b\left\lfloor \frac{a}{b} \right\rfloor$ makes sense for all $a, b \in \mathbb{R}$ and $b \neq 0$. So we can use this to extend the definitions of $x \bmod z$ and the congruence $x \equiv y \pmod{z}$ for $x, y, z \in \mathbb{R}$ with $z \neq 0$ by

$$\begin{aligned} x \equiv y \pmod{z} &\Leftrightarrow x \bmod z = y \bmod z \Leftrightarrow x - z\left\lfloor \frac{x}{z} \right\rfloor = y - z\left\lfloor \frac{y}{z} \right\rfloor \\ &\Leftrightarrow \frac{x-y}{z} = \left\lfloor \frac{x}{z} \right\rfloor - \left\lfloor \frac{y}{z} \right\rfloor. \end{aligned}$$

From this, it is not difficult to see that

$$x \equiv y \pmod{z} \Leftrightarrow \frac{x-y}{z} \text{ is an integer.}$$

For instance, we have $\frac{5}{2} \equiv \frac{1}{2} \pmod{2}$, $\pi \equiv -\pi \pmod{2\pi}$. We will give more properties of the function $x \mapsto \lfloor x \rfloor$ in Chapter 3. However, in this text, we mainly consider the congruence of integers $a, b$ with modulus $m \in \mathbb{N}$. So if we write $a \equiv b \pmod{m}$ or $a \not\equiv b \pmod{m}$, it is assumed that $a$ and $b$ are integers and $m$ is a positive integer. We have the following basic results on congruences.

**Theorem 1.20.** *The following statements hold.*

(i) $a \equiv a \pmod{m}$.

(ii) *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$.

(iii) *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.

(iv) *Assume that* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$. *Then*

$$\begin{aligned} a+c &\equiv b+d \pmod{m}, \\ a-c &\equiv b-d \pmod{m}, \\ ac &\equiv bd \pmod{m}, \\ a^n &\equiv b^n \pmod{m} \textit{ for every } n \in \mathbb{N}, \textit{ and} \\ f(a) &\equiv f(b) \pmod{m} \textit{ for every polynomial } f \textit{ with} \\ &\qquad\qquad \textit{integer coefficients.} \end{aligned}$$

Theorem 1.20 basically tells us that we can perform additions, subtractions, and multiplications on members of two congruences with the same modulus as if they were equations. Nevertheless, we need to be more careful in the division between congruences as shown in the next theorem.

**Theorem 1.21.** *The following statements hold.*

(i) *If* $c > 0$, *then* $a \equiv b \pmod{m}$ *if and only if* $ac \equiv bc \pmod{mc}$.

(ii) *If* $ac \equiv bc \pmod{m}$, *then* $a \equiv b \pmod{\frac{m}{(m,c)}}$. *In particular, if* $(m,c) = 1$ *and* $ac \equiv bc \pmod{m}$, *then* $a \equiv b \pmod{m}$.

(iii) *If* $a \equiv b \pmod{m}$, $k > 0$, *and* $k \mid m$, *then* $a \equiv b \pmod{k}$.

(iv) *If* $a \equiv b \pmod{m}$, *then* $(a,m) = (b,m)$.

(v) *If* $a \equiv b \pmod{m}$*, then the remainder in the division of* $a$ *and* $b$ *by* $m$ *are the same, or equivalently,*

$$a \bmod m = b \bmod m.$$

(vi) *Assume that* $a \equiv b \pmod{m}$ *and* $a \equiv b \pmod{n}$*. Then* $a \equiv b \pmod{[m,n]}$*. In particular, if* $(m,n) = 1$*, then* $a \equiv b \pmod{mn}$*.*

(vii) *If* $a \equiv b \pmod{m}$ *and* $0 \le |a-b| < m$*, then* $a = b$*.*

## 1.6. Residue Systems

A *complete system of residues modulo* $m$ (or a *complete residue system modulo* $m$) is a set of integers such that every integer is congruent modulo $m$ to exactly one member of the set. For example, the sets $\{0, 1, 2, \dots, m-1\}$ and $\{1, 2, \dots, m\}$ are complete residue systems modulo $m$. The first set is called a complete system of least nonnegative residues modulo $m$ and the second set is called a complete system of least positive residues modulo $m$. In addition, $\left(-\frac{m}{2}, \frac{m}{2}\right] \cap \mathbb{Z}$ is also a complete residue system consisting of absolute least residues modulo $m$. In general, we have the following results.

**Theorem 1.22.** *The following statements hold for every* $m \in \mathbb{N}$*.*

(i) *A set of* $m$ *integers that are incongruent modulo* $m$ *forms a complete residue system modulo* $m$*.*

(ii) *If* $\{a_1, a_2, \dots, a_m\}$ *is a complete residue system modulo* $m$ *and* $(k,m) = 1$*, then* $\{ka_1, ka_2, \dots, ka_m\}$ *is also a complete residue system modulo* $m$*.*

For each positive integer $n$, let $\varphi(n)$ be the number of positive integers in $\{1, 2, \dots, n\}$ that are relatively prime to $n$. For example, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(7) = 6$, and $\varphi(10) = 4$. In general, we have $\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$ for every $n \in \mathbb{N}$. The function $\varphi$ is called *Euler's function* and more of its properties will be given in later chapters.

A *reduced residue system modulo* $m$ is a set of integers such that every integer relatively prime to $m$ is congruent modulo $m$ to exactly one member of the set. We have the following results.

**Theorem 1.23.** *The following statements hold for every* $m \in \mathbb{N}$*.*

(i) *A set of* $\varphi(m)$ *integers that are incongruent modulo* $m$ *and are relative to* $m$ *forms a reduced residue system modulo* $m$*.*

(ii) *Assume that* $(k, m) = 1$. *If* $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ *is a reduced residue system modulo* $m$, *then so is the set*

$$\{ka_1, ka_2, \ldots, ka_{\varphi(m)}\}.$$

**Theorem 1.24.** *Let* $m_1$, $m_2$, $d$, *and* $k$ *be positive integers. Then the following statements hold.*

(i) *If* $(m_1, m_2) = 1$, $a_1$ *runs through a complete residue system modulo* $m_1$ *and* $a_2$ *runs through a complete residue system modulo* $m_2$, *then* $a_1m_2 + a_2m_1$ *runs through a complete residue system modulo* $m_1m_2$.

(ii) *If* $(m_1, m_2) = 1$, $a_1$ *runs through a reduced residue system modulo* $m_1$ *and* $a_2$ *runs through a reduced residue system modulo* $m_2$, *then* $a_1m_2 + a_2m_1$ *runs through a reduced residue system modulo* $m_1m_2$.

(iii) *If* $d \mid k$ *and* $(a, d) = 1$, *then the number of elements in the set*

$$\{a + td \mid t = 1, 2, 3, \ldots, k/d\}$$

*that are relatively prime to* $k$ *is* $\varphi(k)/\varphi(d)$.

(iv) *Let* $S$ *be a reduced residue system modulo* $k$ *and* $d \mid k$. *Then we have the following decompositions of* $S$:

   (a) $S$ *is the union of* $\varphi(k)/\varphi(d)$ *disjoint sets, each of which is a reduced residue system modulo* $d$.

   (b) $S$ *is the union of* $\varphi(d)$ *disjoint sets, each of which consists of* $\varphi(k)/\varphi(d)$ *numbers congruent to each other modulo* $d$.

**Proof.** The proof of (i) and (ii) is given in Hardy and Wright [**179**, pp. 63–64]. The statements (iii) and (iv) are given in Apostol [**18**, pp. 124–125]. We leave the details to the reader. ☐

An extension of Theorem 1.24 is given in Exercise 1.13.12.

## 1.7. Chinese Remainder Theorem

Let $a, b$ be integers and let $m$ be a positive integer. A congruence of the form

$$ax \equiv b \pmod{m} \tag{1.1}$$

is called a *linear congruence in one variable*. If $x_0$ is a solution to (1.1), then any integer belonging to the residue class of $x_0$ modulo $m$ is also a solution to (1.1). So if (1.1) has a solution, then it has infinitely many solutions in $\mathbb{Z}$. Nevertheless, it is conventional to count the solutions to (1.1) in $\mathbb{Z}/m\mathbb{Z}$ rather than in $\mathbb{Z}$. Thus solutions belonging to the same residue class are not counted as distinct. Then we have the following result.

**Theorem 1.25.** *Let $a, b$, and $m$ be integers, $m > 0$, and $d = (a, m)$. Consider the congruence $ax \equiv b \pmod{m}$. If $d \nmid b$, then it has no solution. If $d \mid b$, then it has exactly $d$ solutions incongruent modulo $m$. In this case, if $x_0$ is a solution, then all incongruent solutions are given by $x \equiv x_0 + \frac{m}{d}t \pmod{m}$ where $t = 0, 1, 2, \ldots, d-1$.*

By Theorem 1.25, if $(a, m) = 1$, then the congruence

$$ax \equiv b \pmod{m}$$

has a unique solution modulo $m$. If $x$ is the solution to

$$ax \equiv 1 \pmod{m},$$

then $x$ is called an *inverse of $a$ modulo $m$*.

We next give the Chinese remainder theorem which concerns the solution to a system of linear congruences in one variable.

**Theorem 1.26.** (Chinese remainder theorem) *Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers and let $M = m_1 m_2 \cdots m_r$. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

*has a unique solution modulo $M$. The solution is explicitly given by*

$$x \equiv a_1 M_1 M_1' + a_2 M_2 M_2' + \cdots + a_r M_r M_r' \pmod{M},$$

*where $M_i = \frac{M}{m_i}$ and $M_i'$ is the inverse of $M_i$ modulo $m_i$ for each $i = 1, 2, \ldots, r$.*

If the moduli are not pairwise relatively prime, then we can use the following two theorems instead. We first give an answer for the system of two congruences. Then we will use it to provide a solution for the system of any number of congruences.

**Theorem 1.27.** *The system of congruences*

$$x \equiv a_1 \pmod{m_1}, \ x \equiv a_2 \pmod{m_2}$$

*has a solution if and only if* $a_1 - a_2$ *is divisible by* $(m_1, m_2)$. *If there is a solution, it is unique modulo* $[m_1, m_2]$.

**Proof.** Let $d = (m_1, m_2)$. Suppose that there is an integer $x$ satisfying both congruences. Then $x \equiv a_1 \pmod{d}$ and $x \equiv a_2 \pmod{d}$. Therefore $a_1 \equiv a_2 \pmod{d}$, as required. Conversely, suppose $a_1 - a_2$ is divisible by $d$. Let $x = a_1 + m_1 q$ for an integer $q$ to be determined later. Then $x \equiv a_1 \pmod{m_1}$. So we only need to find $q$ such that $a_1 + m_1 q \equiv a_2 \pmod{m_2}$. This is equivalent to

$$\frac{m_1}{d} q \equiv \frac{a_2 - a_1}{d} \pmod{\frac{m_2}{d}}.$$

Since $(m_1/d, m_2/d) = 1$, there exists an integer $q$ satisfying the above congruence. With this $q$, we see that $x$ is a required solution to both congruences. Next, suppose $x$ and $y$ are the solutions. Then

$$x \equiv y \pmod{m_1} \text{ and } x \equiv y \pmod{m_2}.$$

So $m_1$ and $m_2$ divide $x - y$. Therefore $[m_1, m_2]$ divides $x - y$. This completes the proof. □

We can extend Theorem 1.27 to more than two congruences by induction as shown below.

**Theorem 1.28.** *Consider the system of congruences*

$$x \equiv a_i \pmod{m_i} \quad \textit{for } i = 1, 2, 3, \ldots, r.$$

*This system has a solution if and only if* $(m_i, m_j)$ *divides* $a_i - a_j$ *for all pairs* $i, j = 1, 2, 3, \ldots, r$. *If a solution exists, then it is unique modulo* $[m_1, m_2, \ldots, m_r]$.

**Proof.** Let $x$ be a solution to the above system of congruences. Let $1 \le i < j \le r$ and $d = (m_i, m_j)$. Since

$$x \equiv a_i \pmod{m_i}, \quad x \equiv a_j \pmod{m_j},$$

and $d$ divides both $m_i$ and $m_j$, we obtain

$$x \equiv a_i \pmod{d} \quad \text{and} \quad x \equiv a_j \pmod{d}.$$

Therefore $a_i \equiv a_j \pmod{d}$, as required. Next, we prove the converse by induction on $r$. If $r = 1$, then the result is obvious. If $r = 2$, then it is the same as Theorem 1.27. So let $r \geq 3$ and assume that the result holds for $1, 2, 3, \ldots, r-1$. Assume also that $a_i - a_j$ is divisible by $(m_i, m_j)$ for all $i, j = 1, 2, \ldots, r$. By the induction hypothesis, the system of congruences $x \equiv a_i \pmod{m_i}$ for all $i = 1, 2, \ldots, r-1$ has a solutions, say

$$x \equiv x_0 \pmod{[m_1, m_2, \ldots, m_{r-1}]}. \tag{1.2}$$

So it remains to find $x$ satisfying (1.2) and $x \equiv a_r \pmod{m_r}$. By Theorem 1.27, such an $x$ exists if and only if $x_0 - a_r \equiv 0 \pmod{M}$, where $M = ([m_1, m_2, \ldots, m_{r-1}], m_r)$. By Theorem 1.16, it is not difficult to see that

$$M = [(m_1, m_r), (m_2, m_r), \ldots, (m_{r-1}, m_r)].$$

Therefore we only need to show that

$$x_0 - a_r \equiv 0 \pmod{(m_i, m_r)} \quad \text{for every } i = 1, 2, \ldots, r-1.$$

So let $1 \leq i \leq r-1$ and $d = (m_i, m_r)$. We have $a_i \equiv a_r \pmod{d}$. In addition, $x_0 \equiv x \equiv a_i \pmod{m_i}$, and so $x_0 \equiv a_i \pmod{d}$. Therefore $x_0 - a_r \equiv a_i - a_r \equiv 0 \pmod{d}$, as required. So the proof of the converse is complete. For the second statement, if $x$ and $y$ are the solutions to the system of congruences, then $x \equiv y \pmod{m_i}$ for all $i$, which implies the desired result. This completes the proof. □

A linear congruence may appear in two or more variables too. Here we only give a simple result but more information can be found in, for example, Chapter 4 of the book by Rosen [**348**] and Chapter 2 of Niven, Zuckerman, and Montgomery [**290**].

**Theorem 1.29.** *Let $a, b, c, m \in \mathbb{Z}$, $m > 0$, and let $d = (a, b, m)$. The congruence in two variables $ax + by \equiv c \pmod{m}$ has a solution if and only if $d \mid c$.*

**Proof.** If there is a solution, then there are $x, y, q \in \mathbb{Z}$ such that $ax + by = c + mq$, which implies $d \mid c$. Suppose that $d \mid c$. Let $c = dq_0$ for some $q_0 \in \mathbb{Z}$. Since $(a, b, m) = d$, there are integers $x$, $y$, $z$ such that $ax + by + mz = d$. Then $axq_0 + byq_0 \equiv c \pmod{m}$. So $x_0 = xq_0$ and $y_0 = yq_0$ is a solution. This completes the proof. □

An extension of Theorem 1.29 is given in Exercise 1.13.11.

## 1.8. Polynomial and Some Special Congruences

A congruence of the form $f(x) \equiv 0 \pmod{m}$ where $f$ is a polynomial with integer coefficients is called a *polynomial congruence*. If $a$ satisfies $f(a) \equiv 0 \pmod{m}$, then $a$ is called a root of $f$ modulo $m$. The reader interested in finding the solutions of polynomial congruences or basic Diophantine equations is referred to Apostol [**18**], Andreescu, Andrica, and Cucurezeanu [**10**], Andreescu and Andrica [**9**], Niven, Zuckerman, and Montgomery [**290**], and Stillwell [**386**]. However, we do not need such results in this text, and therefore we recall only some well-known theorems of Euler, Lagrange, Fermat, and Wilson. As usual, we write $\mathbb{Z}[x]$ for the set of all polynomials in $x$ with integer coefficients. We have the following results.

(Lagrange's Theorem) If $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree $n \geq 1$ and $p$ is a prime, then $f(x)$ has at most $n$ incongruent roots modulo $p$.

(Fermat's Little Theorem) If $p$ is a prime, then $a^p \equiv a \pmod{p}$ for any $a \in \mathbb{Z}$.

(Euler's Theorem) If $a \in \mathbb{Z}$, $m \in \mathbb{N}$, and $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

(Wilson's Theorem) If $p$ is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

(The Converse of Wilson's Theorem) If $n \geq 2$ and

$$(n-1)! \equiv -1 \pmod{n},$$

then $n$ is a prime. In fact, if $n$ is composite and $n \geq 5$, then

$$(n-1)! \equiv 0 \pmod{n}.$$

Lagrange's theorem can be proved by induction on the degree of $f(x)$. Euler's and Wilson's theorems follow from an application of a reduced residue system. Fermat's little theorem can be obtained from Euler's theorem. The details are as follows.

**Proof of Lagrange's theorem.** If $f(x) = a_1x + a_0$ and $p \nmid a_1$, then $a_1x + a_0 \equiv 0 \pmod{p}$ has exactly one solution, namely

$$x \equiv -a_1^{-1}a_0 \pmod{p},$$

where $a_1^{-1}$ is the inverse of $a_1$ modulo $p$. Next let $n \geq 2$ and assume that the result holds for all polynomials of degree $n-1$. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_i \in \mathbb{Z}$ for every $i$ and $a_n$ is not divisible by $p$. Suppose for a contradiction that $f(x)$ has $n+1$ incongruent roots modulo $p$, say $x_0, x_1, \ldots, x_n$. Then by a straightforward calculation, we have

$$f(x) - f(x_0) = (x - x_0)g(x) \text{ where } g(x) \in \mathbb{Z}[x] \text{ has degree } n-1.$$

This implies that $g(x_k) \equiv 0 \pmod{p}$ for all $k = 1, 2, \ldots, n$. So $g(x)$ has at least $n$ incongruent roots modulo $p$, contradicting the induction hypothesis. ☐

**Proof of Euler's theorem.** Suppose $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ is a reduced residue system mod $m$. Then $\{aa_1, aa_2, \ldots, aa_{\varphi(m)}\}$ is also a reduced residue system mod $m$. Therefore

$$\begin{aligned} a^{\varphi(m)}a_1a_2\cdots a_{\varphi(m)} &= (aa_1)(aa_2)\cdots(aa_{\varphi(m)}) \\ &\equiv a_1a_2\cdots a_{\varphi(m)} \pmod{m}. \end{aligned}$$

Canceling $a_1a_2\cdots a_{\varphi(m)}$ gives the desired result. ☐

**Proof of Fermat's little theorem.** If $p \nmid a$, then Euler's theorem implies that $a^{p-1} \equiv 1 \pmod{p}$, and multiplying by $a$ on both sides gives the desired result. If $p \mid a$, then both sides are zero mod $p$. ☐

**Proof of Wilson's theorem.** When $p = 2$ or $3$, the result is easily checked. So assume that $p \geq 5$. Recall that if $(a, p) = 1$, then there exists $x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{p}$. In addition, $a^2 \equiv 1 \pmod{p}$ if and only if $a \equiv 1, -1 \pmod{p}$. Therefore for each $a$ in $\{2, 3, \ldots, p-2\}$, there exists $b \in \{2, 3, \ldots, p-2\}$ such that $a \neq b$ and $ab \equiv 1 \pmod{p}$. This implies that $(2)(3)\cdots(p-2) \equiv 1 \pmod{p}$. Hence $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$. ☐

**Proof of the converse of Wilson's theorem.** Assume that $n$ is composite and $n \geq 5$. Then $n = ab$ where $1 < a \leq b < n$. If $a \neq b$, then $(n-1)!$ can be written as $(1)(2)\cdots(a)\cdots(b)\cdots(n-1)$ which is divisible by $ab = n$. So suppose $a = b$. Then $n = a^2$. Since $n \geq 5$, $a \geq 3$. Therefore $a^2 - 1 > 2a$. Then we can write $(n-1)!$ as a product from 1 to $a^2 - 1$, which has $a$ and $2a$ as factors. So it is divisible by $a^2 = n$. This completes the proof. ☐

**Alternative proof of the converse of Wilson's theorem.**

Suppose that $(n-1)!+1 \equiv 0 \pmod{n}$ but $n$ is composite. Then there is an integer $a$ such that $1 < a < n$ and $a \mid n$. Since $a < n, a \mid (n-1)!$. We also have $a \mid n$ and $n \mid (n-1)!+1$. So $a \mid (n-1)!+1$. This implies $a \mid 1$. So $a = 1$, a contradiction.

Wolstenholme's theorem and Gauss' generalization of Wilson's theorem are well known and may be useful in solving some exercises. We state them below and refer the reader to Hardy and Wright [**179**, pp. 112–114 and pp. 132–134] for the proof.

**Theorem 1.30.** (Wolstenholme's Theorem) *Let* $p \geq 5$ *and* $H(p-1) = \sum_{k=1}^{p-1} \frac{1}{k}$. *Then* $p^2$ *divides the numerator of* $H(p-1)$ *when it is written in reduced form. Equivalently,*

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2} \text{ for every prime } p \geq 5.$$

**Theorem 1.31.** (Gauss) *Let* $n$ *be a positive integer and let* $g(n)$ *be the product of all positive integers* $m \leq n$ *such that* $(m,n) = 1$. *Then*

$$g(n) \equiv \begin{cases} -1 \pmod{n}, & \text{if } n = 2, 4, p^a, 2p^a \text{ for some } a \geq 1 \text{ and} \\ & \text{odd prime } p; \\ 1 \pmod{n}, & \text{otherwise.} \end{cases}$$

*In other words,* $g(n) \equiv -1 \pmod{n}$ *if* $n$ *has a primitive root, and* $g(n) \equiv 1 \pmod{n}$ *otherwise.*

For some generalizations of factorials, see for example, the articles by Bhargava [**53**], and by Cosgrave and Dilcher [**93**]. Other basic results concerning polynomial congruences are given below. For the proof, see Niven, Zuckerman, and Montgomery[**290**, pp. 87-89 and pp. 94–101].

**Theorem 1.32.** (Hensel's Lemma) *Suppose* $f(x)$ *is a polynomial with integer coefficients. If* $f(a) \equiv 0 \pmod{p^j}$ *and* $f'(a) \not\equiv 0 \pmod{p}$, *then there is a unique* $t \pmod{p}$ *such that* $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$.

**Theorem 1.33.** *Let* $f(x)$ *be a polynomial with integer coefficients. Suppose that* $f(a) \equiv 0 \pmod{p^j}$, *that* $p^\tau \parallel f'(a)$, *and that* $j \geq 2\tau+1$. *If* $b \equiv a \pmod{p^{j-\tau}}$ *then* $f(b) \equiv f(a) \pmod{p^j}$ *and* $p^\tau \parallel f'(b)$. *Moreover, there is a unique* $t \pmod{p}$ *such that* $f(a+tp^{j-\tau}) \equiv 0 \pmod{p^{j+1}}$.

**Theorem 1.34.** *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $n \geq 1$ with leading coefficient* 1. *Then the congruence $f(x) \equiv 0 \pmod{p}$ has $n$ solutions if and only if $f(x)$ is a factor of $x^p - x$ modulo $p$, that is, if and only if $x^p - x = f(x)q(x) + ps(x)$, where $q(x)$ and $s(x)$ have integral coefficients, $q(x)$ has degree $p - n$ and leading coefficient* 1, *and where either $s(x)$ is a polynomial of degree less than $n$ or $s(x)$ is zero.*

**Theorem 1.35.** *If $d \mid (p-1)$, then $x^d \equiv 1 \pmod{p}$ has $d$ solutions.*

**Theorem 1.36.** *If $p$ is a prime and $(a, p) = 1$, then the congruence $x^n \equiv a \pmod{p}$ has $(n, p-1)$ solutions or no solution according to whether $a^{(p-1)/(n,p-1)} \equiv 1 \pmod{p}$ or not.*

## 1.9. Lifting the Exponents

There is a formula for the $p$-adic valuation of the numbers of the form $x^n - y^n$ which are useful in problem solving. This is usually referred to as *lifting the exponent lemma*.

**Theorem 1.37.** (Lifting the Exponent Lemma) *Let $x, y \in \mathbb{Z}$, $n \in \mathbb{N}$, and let $p$ be a prime such that $p \nmid x$ and $p \nmid y$. Then the following statements hold.*

(i) *If $p$ is odd and $p \mid x - y$, then $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$.*

(ii) *If $p$ is odd, $n$ is odd, and $p \mid x + y$, then*

$$v_p(x^n + y^n) = v_p(x + y) + v_p(n).$$

*When $p = 2$ (so $x$ and $y$ are odd integers), we have*

(iii) *if $n$ is odd, then $v_2(x^n - y^n) = v_2(x - y)$ and*

$$v_2(x^n + y^n) = v_2(x + y),$$

(iv) *if $n$ is even, then $v_2(x^n - y^n) = v_2(x^2 - y^2) + v_2(n) - 1$.*

**Proof.** If $n$ is odd, then $x^n + y^n = x^n - (-y^n)$, and so the formulas for $v_p(x^n + y^n)$ follow from those of $v_p(x^n - y^n)$. Therefore (ii) and the second part in (iii) can be respectively obtained from (i) and the first part of (iii). In addition, if $n$ is odd, then

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}). \tag{1.3}$$

We use (1.3) throughout the proof. For (iii), since $x$, $y$, and $n$ are odd, the second factor $x^{n-1} + x^{n-2}y + \cdots + y^{n-1}$ is odd, which implies (iii). For (iv), let $n = 2^a b$ where $a \geq 1$ and $2 \nmid b$. Then by (iii),

$$v_2(x^n - y^n) = v_2\left((x^{2^a})^b - (y^{2^a})^b\right) = v_2\left(x^{2^a} - y^{2^a}\right).$$

We observe that

$$x^{2^a} - y^{2^a} = \left(x^{2^{a-1}} + y^{2^{a-1}}\right)\left(x^{2^{a-2}} + y^{2^{a-2}}\right)\cdots(x^2 + y^2)(x^2 - y^2)$$

and for each $m \geq 1$, $x^{2^m} \equiv y^{2^m} \equiv 1 \pmod 4$ and so

$$x^{2^m} + y^{2^m} \equiv 2 \pmod 4.$$

Therefore

$$v_2\left(x^{2^a} - y^{2^a}\right) = a - 1 + v_2(x^2 - y^2) = v_2(x^2 - y^2) + v_2(n) - 1.$$

It only remains to prove (i). Let $p$ be odd and $p \mid x - y$.

**Case 1** $p \nmid n$. Since $x \equiv y \pmod p$, the second factor on the right side of (1.3) is

$$x^{n-1} + x^{n-2}x + \cdots + x^{n-1} \equiv nx^{n-1} \not\equiv 0 \,(\mathrm{mod}\, p).$$

So $v_p(x^n - y^n) = v_p(x - y) = v_p(x - y) + v_p(n)$.

**Case 2** $p = n$. Then we only need to show that the $p$-adic valuation of the second factor $x^{p-1} + x^{p-2}y + \cdots + y^{p-1}$ is equal to 1. Since $p \mid y - x$, we let $y = x + kp$ where $k \in \mathbb{Z}$. For $1 \leq m \leq p - 1$, we have

$$\begin{aligned} x^{p-1-m}y^m = x^{p-1-m}(x + kp)^m &\equiv x^{p-1-m}\left(x^m + mx^{m-1}kp\right) \\ &\equiv x^{p-1} + kpmx^{p-2} \pmod{p^2}. \end{aligned}$$

This implies that $x^{p-1} + x^{p-2}y + \cdots + y^{p-1}$ is congruent to

$$\begin{aligned} x^{p-1} + \sum_{m=1}^{p-1}(x^{p-1} + kpmx^{p-2}) &\equiv px^{p-1} + \frac{kp^2(p-1)x^{p-2}}{2} \\ &\equiv px^{p-1} \pmod{p^2}. \end{aligned}$$

This implies that $v_p(x^{p-1} + x^{p-2}y + \cdots + y^{p-1}) = 1$, as required.

**Case 3** $n = p^k b$ where $k \geq 1$ and $p \nmid b$. By Case 1, we obtain

$$v_p(x^n - y^n) = v_p\left(\left(x^{p^k}\right)^b - \left(y^{p^k}\right)^b\right) = v_p\left(x^{p^k} - y^{p^k}\right).$$

Applying the result in Case 2 repeatedly, $v_p\left(x^{p^k}-y^{p^k}\right)$ is equal to

$$\begin{aligned} v_p\left((x^{p^{k-1}})^p-(y^{p^{k-1}})^p\right) &= v_p\left(x^{p^{k-1}}-y^{p^{k-1}}\right)+1 \\ &= \cdots = v_p(x-y)+k, \end{aligned}$$

which is $v_p(x-y)+v_p(n)$. So the proof is complete. $\square$

**Remark 1.38.** If $p \mid x$ but $p \nmid y$, then obviously $v_p(x^n-y^n)=0$ for all $n \in \mathbb{N}$. If both $x$ and $y$ are divisible by $p$, then we can take the common factor of $x$ and $y$ before applying the lifting of the exponent lemma. For example, suppose $x$ and $y$ are even, say $x=2^a b$, $y=2^c d$ where $a, c \geq 1$ and $b$, $d$ are odd. If $a>c$, then

$$v_2(x^n-y^n)=v_2\left(2^{cn}\left(2^{an-cn}b^n-d^n\right)\right)=cn.$$

If $a=c$, then $v_2(x^n-y^n)$ is equal to

$$cn+v_2(b^n-d^n)=\begin{cases} cn+v_2(b-d), & \text{if } n \text{ is odd;} \\ cn+v_2(b^2-d^2)+v_2(n)-1, & \text{if } n \text{ is even.} \end{cases}$$

## 1.10. Primitive Roots

Let $a$ and $m$ be relatively prime positive integers. By Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$. So there exists the smallest positive integer $k$ such that $a^k \equiv 1 \pmod{m}$. The integer $k$ is called the *order of $a$ modulo $m$* and is denoted by $\operatorname{ord}_m a$. It is not difficult to show that for $x, y \in \mathbb{N} \cup \{0\}$, we have

$$a^x \equiv a^y \pmod{m} \text{ if and only if } x \equiv y \pmod{\operatorname{ord}_m a}. \tag{1.4}$$

So if $n$ is a positive integer and $a^n \equiv 1 \pmod{m}$, then $\operatorname{ord}_m a \mid n$. In particular, $\operatorname{ord}_m a \mid \varphi(m)$. Therefore $\operatorname{ord}_m a \leq \varphi(m)$. If $\operatorname{ord}_m a=\varphi(m)$, then we say that $a$ is a *primitive root of $m$* (or a *primitive root modulo $m$*). Some properties of the order of $a$ modulo $m$ are the following.

(i) If $a^{-1}$ is the inverse of $a$ modulo $m$, then $\operatorname{ord}_m a^{-1}=\operatorname{ord}_m a$.

(ii) If $a$ is a primitive root of $m$, then the set $\{a, a^2, \ldots, a^{\varphi(m)}\}$ is a reduced residue system modulo $m$.

(iii) If $\operatorname{ord}_m a=k$, then $\operatorname{ord}_m a^n=\frac{k}{(k,n)}$. In particular, if $a$ is a primitive root of $m$, then $a^n$ is a primitive root of $m$ if and only if $(n, \varphi(m))=1$. In addition, if $m$ has a primitive root, then it has exactly $\varphi(\varphi(m))$ incongruent primitive roots modulo $m$.

(iv) If $(b, m) = (a, m) = 1$ and $(\operatorname{ord}_m a, \operatorname{ord}_m b) = 1$, then

$$\operatorname{ord}_m(ab) = (\operatorname{ord}_m a)(\operatorname{ord}_m b).$$

(v) If $a$ is odd and $k \geq 3$, then $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. If $k \geq 2$, then $\operatorname{ord}_{2^k} 5 = 2^{k-2}$.

There are a number of steps in the classification of all positive integers that have a primitive root. Here we only give the statement and refer the reader to the other books such as [**290**] and [**348**] for more details.

**Theorem 1.39.** *Let $n > 1$ be a positive integer. Then $n$ has a primitive root if and only if $n = 2$, $4$, $p^k$ or $2p^k$, where $p$ is an odd prime and $k$ is a positive integer.*

## 1.11. Quadratic Residues

Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$. We say that $a$ is an *nth power residue modulo m* if $a \equiv x^n \pmod{m}$ for some $x \in \mathbb{Z}$. In particular, $a$ is a *quadratic residue modulo m* if there exists $x \in \mathbb{Z}$ such that $a \equiv x^2 \pmod{m}$. If there is no integer $x$ with $a \equiv x^2 \pmod{m}$, then $a$ is said to be *quadratic nonresidue modulo m*. By the Chinese remainder theorem and Hensel's lemma, we usually restrict our attention to the case where $m$ is prime and $(a, m) = 1$. For example, if $m = 7$, $x \in \mathbb{Z}$, and $(x, 7) = 1$, then $x^2 \equiv 1, 2, 4 \pmod{7}$. This shows that 1, 2, and 4 are quadratic residues modulo 7 while 3, 5, and 6 are quadratic nonresidues modulo 7. In dealing with quadratic residues, it is convenient to use the Legendre symbol. Recall that if $p$ is an odd prime and $(a, p) = 1$, then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \equiv x^2 \pmod{p} \text{ for some } x \in \mathbb{Z}; \\ -1, & \text{if } a \not\equiv x^2 \pmod{p} \text{ for any } x \in \mathbb{Z}. \end{cases}$$

For convenience, we also define $\left(\frac{a}{p}\right) = 0$ if $p \mid a$. So, for instance, $\left(\frac{7}{7}\right) = 0$, $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$, and $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$. Now suppose $p$ is an odd prime and $a, b \in \mathbb{Z}$ are not divisible by $p$. Some results concerning quadratic residues of prime numbers are as follows.

(i) There are exactly $(p-1)/2$ quadratic residues of $p$ and $(p-1)/2$ quadratic nonresidues of $p$ among the integers $1, 2, \ldots, p-1$.

(ii) Every primitive root of $p$ is a quadratic nonresidue of $p$.

(iii) (Euler's Criterion) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(iv) (Gauss's Lemma) If $s$ is the number of least positive residues of the integers $a, 2a, 3a, \ldots, ((p-1)/2)a$ that are greater than $p/2$, then $\left(\frac{a}{p}\right) = (-1)^s$.

(v) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(vi) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(vii) $\left(\frac{a^2}{p}\right) = 1$.

(viii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}; \\ -1, & \text{if } p \equiv -1 \pmod{4}. \end{cases}$

(ix) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}.$

(x) (Quadratic Reciprocity Law) If $p$ and $q$ are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

## 1.12. Sum of Squares

We say that $n$ is a sum of two squares if $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. For example, $1 = 1^2 + 0^2$ is a sum of two squares but 3 cannot be written as a sum of two squares. Similarly, $3 = 1^2 + 1^2 + 1^2$ but 7 is not a sum three squares. In general, we have the following results.

(Sum of Two Squares) The following statements hold.

(i) If $n \equiv 3 \pmod{4}$, then $n$ is not a sum of two squares.

(ii) $p \mid x^2 + 1$ for some $x \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

(iii) If $p$ is a prime and $p \equiv 1 \pmod{4}$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. If $p$ is a prime factor of $a^2 + b^2$ and $p \equiv 3 \pmod{4}$, then $p \mid a$ and $p \mid b$.

(iv) If $a$ and $b$ are sums of two squares, then $ab$ can also be written as a sum of two squares. In fact, we have the identity

$$(x^2 + y^2)(r^2 + s^2) = (xr + ys)^2 + (xs - yr)^2.$$

(v) A positive integer $n$ is a sum of two squares if and only if for every prime $p$, if $p \mid n$ and $p \equiv 3 \pmod{4}$, then $v_p(n)$ is even.

Gauss and Legendre independently proved the corresponding result for the sum of three squares and Lagrange completed the theorems by showing that every positive integer is a sum of four squares (some of them may be $0^2$).

(Sum of Three Squares) A positive integer $n$ is a sum of three squares if and only if $n \neq 4^m(8k+7)$ for any nonnegative integer $m$ and $k$.

(Sum of Four Squares) Every positive integer is a sum of four squares.

## 1.13. Exercises

Unless stated otherwise, all variables denote positive integers.

1.13.1 Show that $[a, b, c](ab, ac, bc) = abc$, and that

$$[a, b, c, d](abc, abd, acd, bcd) = abcd,$$

and in general, $[a_1, a_2, \ldots, a_n]M = a_1 a_2 \cdots a_n$, where $M$ is the greatest common divisor of the numbers that are products of any $n-1$ distinct numbers chosen from $a_1, a_2, \ldots, a_n$.

1.13.2 Let $A$ be a nonempty set of nonzero integers and let $D(A)$ be the set of all common divisors of $A$. Show that $D(A)$ is a nonempty finite set.

1.13.3 Prove that every $n \geq 12$ is the sum of two composite numbers.

1.13.4 Prove that if $2^n - 1$ is prime, then $n$ is prime.

1.13.5 Prove that if $2^n + 1$ is prime, then $n$ is a power of 2.

1.13.6 Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence defined by the recurrence relation $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ with the initial values $F_0 = 0$ and $F_1 = 1$. Show that $(F_{n+1}, F_n) = 1$ for all $n \geq 0$.

1.13.7 Let $a, b \in \mathbb{N}$ and $(a, b) = 1$. Prove the following statements.

(i) There exist positive integers $x$ and $y$ such that $ax - by = 1$.

(ii) For every $n > ab$ there exist positive integers $x$ and $y$ such that $n = ax + by$.

(iii) There are no positive integers $x$ and $y$ such that

$$ab = ax + by.$$

1.13.8 If $n > 1$, prove that the sum

$$\sum_{k=1}^{n} \frac{1}{k}$$

is not an integer.

1.13.9 Show that there are infinitely many $n \in \mathbb{N}$ such that $n$, $n+1$, $n+2$ are sums of two squares. Show also that any set of four consecutive integers contain an element that is not a sum of two squares.

1.13.10 Let $n$ be a positive integer and let $s(n)$ be the sum of digits of $n$ in its decimal representation. Show that the following statements hold.

(i) $9 \mid s(n) - n$.

(ii) $s(m+n) \leq s(m) + s(n)$ (subadditivity property).

(iii) $s(mn) \leq \min(ms(n), ns(m))$.

(iv) $s(mn) \leq s(m)s(n)$ (submultiplicativity property).

1.13.11 Let $a, b, c \in \mathbb{Z}, m \in \mathbb{N}$, and $d = (a, b, m)$. Show that if the linear congruence in two variables $ax + by \equiv c \pmod{m}$ has a solution, then it has exactly $dm$ incongruent solutions modulo $m$. Here we say that two solutions $(x_1, y_1)$ and $(x_2, y_2)$ are incongruent modulo $m$ if $x_1 \not\equiv x_2 \pmod{m}$ and $y_1 \not\equiv y_2 \pmod{m}$.

1.13.12 Let $m_1$, $m_2$, …, $m_k$ be pairwise relatively prime positive integers, $M = m_1 m_2 \cdots m_k$, and $M_j = M/m_j$ for $j = 1, 2, \ldots, k$. Show that $a_1M_1 + a_2M_2 + \cdots + a_kM_k$ runs through a complete residue system modulo $M$ when $a_1$, $a_2$, …, $a_k$ run through a complete residue system modulo $m_1$, $m_2$, …, $m_k$, respectively. Show that the result also holds if

$$a_1M_1 + a_2M_2 + \cdots + a_kM_k$$

is replaced by

$$a_1 + a_2m_1 + a_3m_1m_2 + \cdots + a_km_1m_2 \cdots m_{k-1}.$$

## 1.14. Notes

It is not difficult to show that every $n \geq 12$ can be written as a sum of two composite numbers (see Exercise 1.13.3). On the other hand, Goldbach conjectured in 1742 that every even number $n \geq 4$ is a sum of two primes but this problem is open and seems very difficult. Various partial results have been obtained by many mathematicians. Here we mention a few. Vinogradov [**428**] proved that there exists a large number $N$ such that every odd integer $n \geq N$ is a sum of three primes. Then about 76 years later, Helfgott [**184**] showed that we can take $N = 7$. Chen [**81**] obtained the result very close to Goldbach's conjecture by proving that every large even number can be written as a sum of a prime and a number that has at most two prime factors. For more details, we refer the reader to the books by Hua [**202**] and Vaughan [**422**].

Exercise 1.13.4 is connected with *Mersenne primes*, the primes of the form $2^p - 1$ where $p$ is a prime. We know from Euclid's result (Theorem 1.12) that there exist infinitely many primes but we do not know whether or not the number of Mersenne primes is infinite. The sequence of primes and the sequence of those $p$ such that $2^p - 1$ is prime are given, respectively, as A000040 and A000043 in the On-Line Encyclopedia of Integer Sequences (OEIS). Mersenne primes are also strongly related to *perfect numbers*, the positive integers that are equal to the sum of their proper divisors. In other words, if $\sigma(n)$ denotes the sum of all positive divisors of $n$, then $n$ is perfect if and only if $\sigma(n) = 2n$. For instance, 6 and 28 are perfect as

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 \times 6 \quad \text{and}$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \times 28.$$

Euler showed that an even number $n$ is perfect if and only if

$$n = 2^{p-1}(2^p - 1),$$

where $p$ and $2^p - 1$ are primes. We do not know whether or not there are infinitely many even perfect numbers. We cannot find an odd perfect number and we do not have a proof that such a number does not exist either.

As of November 2022, the largest known prime, which is a Mersenne prime, is $2^{82589933} - 1$ and thus the largest known perfect number is $2^{82589932}(2^{82589933} - 1)$. For more information on the search of Mersenne primes, we recommend the reader to follow the Great Internet Mersenne Prime Search (GIMPS). For the list of perfect numbers, see A000396 in OEIS.

Attempting to understand perfect numbers better, mathematicians have studied other closely related concepts: if $\sigma(n) < 2n$, then $n$ is said to be deficient; if $\sigma(n) > 2n$, then $n$ is abundant; if $\sigma(n) = 2n + 1$, then

$n$ is quasiperfect; if $\sigma(n) = 2n - 1$, then $n$ is almost perfect. For more information on this topic, see for example the online databases GIMPS [**157**] and OEIS [**374**].

Sierpiński [**368**] called *n pseudoperfect* if $n$ can be written as a sum of some of its proper divisors. Pollack and Shevelev [**303**] initiated the study of a subclass of pseudoperfect numbers: $n$ is *near-perfect* if $n$ is the sum of all of its proper divisors except one of them; $n$ is *exactly k-near-perfect* if $n$ is expressible as a sum of all of its proper divisors with exactly $k$ exceptions.

Tang, Ren, and Li [**403**] defined the notion of deficient-perfect numbers in a similar way: $n$ is called a *deficient-perfect number with a deficient divisor d* if $d$ is a proper divisor of $n$ and $\sigma(n) = 2n - d$; $n$ is *exactly k-deficient-perfect with deficient divisors* $d_1, d_2, \dots, d_k$ if $d_1, d_2, \dots, d_k$ are distinct proper divisors of $n$ and

$$\sigma(n) = 2n - (d_1 + d_2 + \cdots + d_k).$$

In 2012, Pollack and Shevelev [**303**] showed that if $k$ is fixed and is large enough, then there are infinitely many exactly $k$-near-perfect numbers. A year later, Ren and Chen [**341**] determined all near-perfect numbers $n$ that have $\omega(n) = 2$ and we can see from this classification that all such $n$ are even. Here and throughout this book, $\omega(n)$ denotes the number of distinct prime divisors of $n$. Tang, Ren, and Li [**403**] proved that there is no odd near-perfect number $n$ with $\omega(n) = 3$ and found all deficient-perfect numbers $m$ with $\omega(m) \leq 2$. After that, Tang and Feng [**401**] extended it by showing that there is no odd deficient-perfect number $n$ with $\omega(n) = 3$. Tang, Ma, and Feng [**402**] obtained in 2016 the only odd near-perfect number with $\omega(n) = 4$, namely, $n = 3^4 \cdot 7^2 \cdot 11^2 \cdot 19^2$, while Sun and He [**390**] asserted in 2019 that the only odd deficient-perfect number $n$ with $\omega(n) = 4$ is $n = 3^2 \cdot 7^2 \cdot 11^2 \cdot 13^2$. Cohen et al. [**87**] improved the estimate of Pollack and Shevelev [**303**] on the number of near-perfect numbers $\leq x$. Hence, most results in the literature were devoted to characterizing, only when $k = 1$, the exactly $k$-near-perfect or exactly $k$-deficient-perfect numbers. Chen [**80**] started a slightly new direction by determining all 2-deficient-perfect numbers $n$ with $\omega(n) \leq 2$. Finally, Aursukaree and the author of this book [**21**] have recently proved that the only odd exactly 3-deficient-perfect number with at most two distinct prime factors is $1521 = 3^2 \cdot 13^2$. We also plan to discover more about these numbers in the future.

Exercise 1.13.5 is about Fermat numbers. The number of the form $2^{2^n} + 1$ is prime for $n = 1, 2, 3, 4$ and Fermat believed that it is a prime for all $n$. However, Euler showed that $2^{2^5} + 1$ is composite. By using computer programming, it is known that $2^{2^n} + 1$ is composite for $5 \leq n \leq 21$, and it is conjectured that there are only a finite number of $n$ such that $2^{2^n} + 1$ is prime.

Exercise 1.13.6 is a well known property of the Fibonacci numbers. More problems on these numbers are also given in later chapters. The books by Koshy [**230**] and Vajda [**418**] show various classical results on $F_n$. For more up-to-date information and research problems on $F_n$, its companion Lucas numbers, and other recurrence sequences, we refer the reader to the *Fibonacci Quarterly* and other publications of the Fibonacci Association. The Fibonacci and Lucas sequences are A000045 and A000032 in OEIS, respectively.

Exercise 1.13.7 shows that if $a, b \in \mathbb{N}$ and $(a, b) = 1$, then the largest positive integer that cannot be written as $ax + by$ for some $x, y \in \mathbb{N}$ is $ab$. This problem is actually related to a concept of Frobenius numbers. Suppose that $a_1, a_2, \dots, a_n$ are positive integers and $(a_1, a_2, \dots, a_n) = 1$. Then every positive integer $m$ can be written as $m = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ for some $x_1, x_2, \dots, x_n \in \mathbb{Z}$. If we restrict our attention only to the case when $n \geq 2$ and $x_1, x_2, \dots, x_n$ are nonnegative integers, then there is a finite number of $m \in \mathbb{N}$ that can not be written as $a_1x_1 + a_2x_2 + \cdots + a_nx_n$. The largest such integer is called the Frobenius number of $\{a_1, a_2, \dots, a_n\}$ and is denoted by $g(a_1, a_2, \dots, a_n)$. It is well known that $g(a, b) = ab - a - b$ for all relatively prime positive integers $a, b$. Tripathi [**414**] also obtained in 2017 formulas for $g(a, b, c)$ for all $a, b, c \in \mathbb{N}$ with $(a, b, c) = 1$. However, a general formula for the Frobenius number of more than three variables is not known. For other recent results on Frobenius numbers, see for instance [**284, 346, 385, 413**].

By considering the highest power of 2, we obtain a proof of Exercise 1.13.8. A similar idea can be used to show that the sum $\sum_{m \leq k \leq n} \frac{1}{k}$ is not an integer for any $n > m \geq 1$. Erdös extended this to the sum of reciprocals of positive integers in an arithmetic progression. Belbachir and Khelladi [**42**] generalized Erdös' result further and obtained that for $a, d, k \in \mathbb{N}$ and $k \geq 2$, the sum

$$\frac{1}{a^{\alpha_0}} + \frac{1}{(a+d)^{\alpha_1}} + \cdots + \frac{1}{(a+(k-1)d)^{\alpha_{k-1}}}$$

is never an integer for all positive rational numbers $\alpha_0, \alpha_1, \dots, \alpha_{k-1}$. In fact, the reciprocal sum of an integer sequence is of general interest in mathematics and theoretical physics as proposed by Bayless and Klyve [**39**], and by Roggero, Nardelli, and Di Noto [**347**]. See also the work of Nguyen and Pomerance [**288**] on the reciprocal sum of the amicable numbers, the preprint of Kinlaw, Kobayashi, and Pomerance [**226**] on the reciprocal sum of the positive integers $n$ satisfying $\varphi(n) = \varphi(n+1)$, the article by Lichtman [**244**] on the reciprocal sum of primitive nondeficient numbers, and the recent paper by Phunphayap and Pongsriiam [**295**] on the reciprocal sum of $b$-adic palindromes. Here amicable numbers are the pairs of positive integers $m, n$ such that $\sigma(m) = \sigma(n) = m+n$; $\varphi$ is the Euler function, and $b$-adic palindromes are the positive integers $n$ such that the representation of $n$ in base $b$ reads the same backward as forward. There are actually many results in the literature concerning sums of unit fractions and we refer the reader to [**19**, **94**, **112**, **148**–**150**, **408**] and references therein for more information.

Let $A_k$ be the set of positive integers $n$ such that $n$, $n+1$, …, $n+k-1$ are sums of two squares. By Exercise 1.13.9, we know that $A_k$ is an infinite set for $k = 1, 2, 3$ and that $A_k = \emptyset$ for all $k \geq 4$. The integers in $A_1, A_2$, and $A_3$ are given, respectively, as sequences A001481, A140612, and A082982 in OEIS. In 1908, Landau [**239**] showed that the number of positive integers $\leq x$ that are a sum of two squares is asymptotic to $\frac{cx}{\sqrt{\log x}}$ where $c$ is an explicitly given constant. That is,

$$A_1(x) := \sum_{\substack{n \leq x \\ n \in A_1}} 1 \sim \frac{cx}{\sqrt{\log x}}. \tag{1.5}$$

The concept of asymptotic relations will be explained in Chapter 3 but for now the reader can think of it as a good approximation. So (1.5) basically says that the left-hand side of (1.5) can be well approximated by $\frac{cx}{\sqrt{\log x}}$. In the following discussion, $c$ with or without subscripts denotes a positive constant which does not depend on $n$ or $x$. Rieger [**345**] showed in 1965 that there exists a constant $c_1 > 0$ such that for all $x \geq 2$

$$A_2(x) := \sum_{\substack{n \leq x \\ n \in A_2}} 1 \leq \frac{c_1 x}{\log x}.$$

About nine years later, Hooley [**191**,**192**] and Indlekofer [**207**] using different methods established that there is a constant $c_2 > 0$ such that

$$A_2(x) := \sum_{\substack{n\le x\\ n\in A_2}} 1 \ge \frac{c_2 x}{\log x}$$

for all $x \ge 2$. Therefore we say that the order of magnitude of $A_2(x)$ is $x/\log x$ and write $A_2(x) \asymp x/\log x$ for $x \ge 2$. Then in 1987, Cochrane and Dressler [**86**] used Selberg's sieve to obtain an upper bound

$$A_3(x) := \sum_{\substack{n\le x\\ n\in A_3}} 1 \le \frac{c_3 x}{(\log x)^{\frac{3}{2}}}.$$

However, the order of magnitude of $A_3(x)$ is not known. Although topics on squares might seem easy, they actually contain many open and difficult questions. Here we mention but a few. Let $(a_n)_{n\ge1} = (1, 2, 4, 5, 8, \ldots)$ be the increasing sequence of positive integers that can be written as a sum of two squares. In 1974, Bambah and Chowla [**28**] showed that there exists a constant $c_4 > 0$ such that for all $n \ge 1$, $a_{n+1} - a_n \le c_4 a_n^{1/4}$ and they believed that the exponent of the upper bound should be improved to a number smaller than 1/4 but it is still unsolved. Refining Lagrange's four-square theorem, Sun [**388**] showed that every positive integer can be written as $x^2 + y^2 + z^2 + w^2$ where $x, y, z, w \in \mathbb{Z}$ and $x+y+z$ is a square. He also posed several conjectures in his article [**388**] and on his homepage [**389**]. For example, his 1-3-5 conjecture states that any positive integer can be written as the sum of four squares of nonnegative integers $x, y, z, w$ such that $x + 3y + 5z$ is also a square. He has offered 1,350 US dollars for the first solution to this problem, but it is still open. For partial answers, see the recent article by Wu and Sun [**438**]. Finally, a famous conjecture on the existence of primes between squares states that for each $n \in \mathbb{N}$, there is a prime $p$ lying between $n^2$ and $(n+1)^2$. This has been verified by using a computer for $n \le 10^6$ but we can neither find a proof nor a counterexample.

Exercise 1.13.10 gives elementary properties of the sum of digits function and is easy to prove. However, the study of this function is not trivial. In fact, there are many interesting questions concerning this function; see for example, Gelfond's sum of digits problems as collected in Morgenbesser's thesis [**276**] and references therein.

It is well known that $(a, b)[a, b] = ab$ for every $a, b \in \mathbb{N}$, and generalizations of this are given in Theorem 1.17 and Exercise 1.13.1, respectively. The $\gcd(A)$ for any nonempty set $A$ of nonzero integers is introduced at the end of Section 1.2 and in Exercise 1.13.2. If $\gcd(A) = 1$, then $A$ is said to be a relatively prime set and if $\gcd(a_1, a_2) = 1$ for every distinct pair $a_1, a_2 \in A$, then $A$ is called a pairwise relatively prime set. A similar concept was introduced by Erdös: $A$ is called a primitive set if $a \nmid b$ for any distinct elements $a, b \in A$. So if $A$ is the empty set or a singleton set, then $A$ is a primitive set and if $|A| \geq 2$, then $1 \notin A$.

The number $f(n)$ of relatively prime subsets of $\{1, 2, \ldots, n\}$ was given by Nathanson [**282**] and generalized by various researchers including the author of this book. The sequence $(f(n))_{n\geq 1}$ is listed as A085945 in OEIS. See also A027375, A038199, and A224840 for related sequences. For more information on this topic, we refer the reader to Pongsriiam [**313–315**] and references therein.

On the other hand, a conjecture of Cameron and Erdös [**72**] on the number $g(n)$ of primitive subsets of $\{1, 2, \ldots, n\}$ has recently been solved by Angelo [**16**]. That is, $\lim_{n\to\infty} g(n)^{\frac{1}{n}}$ exists. There are other interesting theorems on primitive sets too. For instance, by Besicovitch's result [**52**], we know that the upper asymptotic density of a primitive set can be arbitrarily close to 1/2 while the lower asymptotic density is always 0. The reciprocal sum of the elements of a primitive set can diverge but Erdös [**114**] showed that for any primitive set $A \subseteq \mathbb{N} \setminus \{1\}$,

$$\sum_{a\in A} \frac{1}{a \log a} \quad \text{converges.}$$

In fact, the proof shows that the sums are uniformly bounded on all primitive sets $A \subseteq \mathbb{N} \setminus \{1\}$. In fact, Erdös conjectured that for any primitive set $A \subseteq \mathbb{N} \setminus \{1\}$, we have

$$\sum_{a\in A} \frac{1}{a \log a} \leq \sum_{p} \frac{1}{p \log p},$$

where $p$ runs over all prime numbers. Lichtman and Pomerance [**246**] made some contributions, and Lichtmann [**245**] has recently solved this problem.

## Chapter 2

# Arithmetic Functions I

### 2.1. Introduction

An *arithmetic function* (or a *number-theoretic function*) is a complex-valued function defined on the set of positive integers. In this section, we give the definitions of certain arithmetic functions which play an important role in the study of divisibility properties of integers and the distribution of prime numbers. Then we focus our attention on functions which have multiplicative properties, a concept to be defined in Section 2.2. We introduce in Section 2.3 the concept of Dirichlet convolution which enables us to prove various identities in Sections 2.4 and 2.5. Although many results in this chapter are known to undergraduate students, our presentation here is new. In particular, reading the definitions and proofs will help the readers get familiar with elementary calculations in analytic number theory.

**Definition 2.1.** The functions $\varphi, d, \sigma, 1, N, e, \mu, \lambda : \mathbb{N} \to \mathbb{C}$ are defined by

$$\begin{aligned}
\varphi(n) &= \text{ the number of integers } k \text{ such that } 1 \le k \le n \text{ and } (k,n) = 1,\\
d(n) &= \text{ the number of positive divisors of } n,\\
\sigma(n) &= \text{ the sum of positive divisors of } n,\\
1(n) &= 1 \text{ for every } n \in \mathbb{N},\\
N(n) &= n \text{ for every } n \in \mathbb{N},
\end{aligned}$$

$$e(n) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n > 1, \end{cases}$$

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^k, & \text{if } n = p_1 p_2 \cdots p_k \text{ where } p_1, p_2, \dots, p_k \text{ are} \\ & \quad \text{distinct primes;} \\ 0, & \text{if } p^2 \mid n \text{ for some prime } p, \end{cases}$$

$$\lambda(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^{a_1 + a_2 + \cdots + a_k}, & \text{if } n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ where } p_1, p_2, \dots, p_k \\ & \text{are distinct primes and } a_1, a_2, \dots, a_k \\ & \text{are positive integers.} \end{cases}$$

The functions $\varphi$, $d$, $\mu$, and $\lambda$ are called the *Euler function*, the *divisor function*, the *Möbius function*, and *Liouville's function*, respectively. In fact, $d(n)$ and $\sigma(n)$ are special cases of $\sigma_s(n)$ which is the sum of $d^s$ where $d$ ranges over the positive divisors of $n$. So $\sigma_0 = d$ and $\sigma_1 = \sigma$. Nevertheless, we only focus on $d$ and $\sigma$. The functions 1 and $N$ are the identities for the pointwise multiplication of arithmetic functions and the composition of functions which maps from $\mathbb{N}$ to $\mathbb{N}$, respectively. The function $e$ is the identity for the Dirichlet product, a concept to be defined in Section 2.3. Although we use the symbols 1 and $e$ for the functions and for the numbers, there should be no confusion as the context will clearly indicate which is which. It is often more convenient to write the definitions of these functions using summation notation such as

$$\varphi(n) = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} 1, \quad d(n) = \sum_{k \mid n} 1, \quad \sigma(n) = \sum_{d \mid n} d, \quad \text{and} \quad \sigma_s(n) = \sum_{d \mid n} d^s.$$

Here is an example of values of the functions defined in Definition 2.1.

| $n$: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\varphi(n)$: | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 |
| $d(n)$: | 1 | 2 | 2 | 3 | 2 | 4 | 2 | 4 | 3 | 4 |
| $\sigma(n)$: | 1 | 3 | 4 | 7 | 6 | 12 | 8 | 15 | 13 | 18 |
| $1(n)$: | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $N(n)$: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $e(n)$: | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $\mu(n)$: | 1 | -1 | -1 | 0 | -1 | 1 | -1 | 0 | 0 | 1 |
| $\lambda(n)$: | 1 | -1 | -1 | 1 | -1 | 1 | -1 | -1 | 1 | 1 |

The von Mangoldt function $\Lambda$, although it is not multiplicative, plays a central role in the study of the distribution of prime numbers. The functions $\omega$ and $\Omega$ also appear often in the study of primes. Here are their definitions.

**Definition 2.2.** For each integer $n \geq 1$,

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k \text{ for some prime } p \text{ and a positive integer } k; \\ 0, & \text{if } n \text{ is not a power of primes,} \end{cases}$$

$$\omega(n) = \text{ the number of distinct prime divisors of } n,$$

$$\Omega(n) = \text{ the number of prime divisors of } n \text{ counted with multiplicity.}$$

In other words, $\omega(n) = \sum_{p|n} 1$ and $\Omega(n) = \sum_{p^k \| n} k = \sum_{p^k | n} 1$.

Here is a short list of values of $\Lambda(n)$, $\omega(n)$, and $\Omega(n)$.

| $n$: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\Lambda(n)$: | 0 | $\log 2$ | $\log 3$ | $\log 2$ | $\log 5$ | 0 | $\log 7$ | $\log 2$ | $\log 3$ | 0 |
| $\omega(n)$: | 0 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 2 |
| $\Omega(n)$: | 0 | 1 | 1 | 2 | 1 | 2 | 1 | 3 | 2 | 2 |

We observe that $\lambda(n) = (-1)^{\Omega(n)}$ and if $n$ is squarefree, then

$$\omega(n) = \Omega(n) \text{ and } \lambda(n) = (-1)^{\omega(n)} = \mu(n).$$

Since $\omega(1) = \Omega(1) = \Lambda(1) = 0$, these functions are not multiplicative (see Theorem 2.5). Nevertheless, they have some desirable properties similar to multiplicativity.

**Definition 2.3.** Let $f$ be an arithmetic function. We say that $f$ is *additive* if $f(mn) = f(m)+f(n)$ for every $m, n \in \mathbb{N}$ with $(m, n) = 1$. Furthermore, if $f(mn) = f(m) + f(n)$ for all $m, n \in \mathbb{N}$, then $f$ is said to be *completely additive*. If $f$ is additive and $f(p^a) = f(p)$ for all primes $p$ and positive integers $a$, then $f$ is *strongly additive*.

Therefore $\Omega$ is completely additive, $\omega$ is strongly additive, and $\Lambda$ is not additive, but it satisfies $\Lambda(p^a) = \Lambda(p)$. The logarithm function is completely additive and if $f$ is positive and multiplicative, then the function $g$ defined by $g(n) = \log f(n)$ is additive. The verification is left as an exercise to the reader (see Exercises 2.6.1 and 2.6.2). Nevertheless, in this chapter, we focus our attention on multiplicative functions.

## 2.2. Multiplicative Functions

A class of arithmetic functions which play an important role in multiplicative number theory is that of multiplicative functions. The main interest is that they respect the multiplicative structure of $\mathbb{N}$ in the sense that the image of an integer is the product of the images of the prime powers arising in its canonical factorization. The precise definition and results are as follows.

**Definition 2.4.** Let $f$ be an arithmetic function. We say that $f$ is *multiplicative* if $f$ is not identically zero and $f(mn) = f(m)f(n)$ for every $m, n \in \mathbb{N}$ with $(m, n) = 1$. If in addition, $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$, then $f$ is said to be *completely multiplicative*. If $f$ is multiplicative and $f(p^a) = f(p)$ for all primes $p$ and integers $a \geq 1$, then $f$ is *strongly multiplicative*. The set of all multiplicative functions is denoted by $\mathcal{M}$.

**Theorem 2.5.** *If $f$ is multiplicative, then $f(1) = 1$.*

**Proof.** Since $f$ is not identically zero, there exists $n \in \mathbb{N}$ such that $f(n) \neq 0$. Then $f(n) = f(1 \cdot n) = f(1)f(n)$, which implies $f(1) = 1$. □

**Theorem 2.6.** *Let $f$ be an arithmetic function with $f(1) = 1$. Then the following statements hold.*

2.2.1 *$f$ is multiplicative if and only if for all distinct primes $p_i$ and all integers $a_i \geq 0$,*

$$f(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_r^{a_r}). \tag{2.1}$$

2.2.2 *Assume that $f$ is multiplicative. Then $f$ is completely multiplicative if and only if for all primes $p$ and all integers $a \geq 0$,*

$$f(p^a) = f(p)^a. \tag{2.2}$$

**Proof.** The direct part of (i) follows from the fact that $p_1^{a_1}, p_2^{a_2}, \ldots, p_r^{a_r}$ are pairwise relatively prime. For the converse of (i), assume that (2.1) holds. Let $m, n \in \mathbb{N}$ and $(m, n) = 1$. We write $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $n = q_1^{b_1} q_2^{b_2} \cdots q_\ell^{b_\ell}$ in the canonical forms as discussed in Remark 1.14. This includes the case $m = 1$ or $n = 1$ since we allow the $a_i$ and $b_j$ to be zero. In addition, since $(m, n) = 1$, we can assume that the $p_i$ and $q_j$ are all distinct. Therefore we obtain by (2.1) that

$$\begin{aligned} f(mn) &= f\left(p_1^{a_1}\right) f\left(p_2^{a_2}\right) \cdots f\left(p_r^{a_r}\right) f\left(q_1^{b_1}\right) f\left(q_2^{b_2}\right) \cdots f\left(q_\ell^{b_\ell}\right) \\ &= f(m) f(n). \end{aligned}$$

For (ii), it is enough to prove the converse as the other part follows immediately from the definition. So assume that (2.2) holds and $m, n \in \mathbb{N}$. It is convenient to write $m$ and $n$ in the forms (see Remark 1.14)

$$m = \prod_{i=1}^{\infty} p_i^{a_i} \text{ and } n = \prod_{i=1}^{\infty} p_i^{b_i}.$$

Then $mn = \prod p_i^{a_i + b_i}$, and by the multiplicative property of $f$ and by (2.2), we obtain that $f(mn)$ is equal to

$$\begin{aligned} \prod_{i=1}^{\infty} f\left(p_i\right)^{a_i + b_i} &= \prod_{i=1}^{\infty} f\left(p_i\right)^{a_i} \prod_{i=1}^{\infty} f\left(p_i\right)^{b_i} \\ &= \prod_{i=1}^{\infty} f\left(p_i^{a_i}\right) \prod_{i=1}^{\infty} f\left(p_i^{b_i}\right) = f(m) f(n). \end{aligned}$$ □

**Corollary 2.7.** *Let $f$ and $g$ be multiplicative functions. If $f(p^a) = g(p^a)$ for each prime $p$ and positive integer $a$, then $f(n) = g(n)$ for all $n \in \mathbb{N}$.*

**Proof.** The converse is obvious. For the other direction, if $n = \prod_{i=1}^{\infty} p_i^{a_i}$, then by Theorem 2.6, we have

$$f(n) = \prod_{i=1}^{\infty} f(p_i^{a_i}) = \prod_{i=1}^{\infty} g(p_i^{a_i}) = g(n).$$ □

It is easy to check that the functions $e$, $1$, $N$, and Liouville's function given in Definition 2.1 are completely multiplicative and the others are not.

Recall that $d(1) = 1$ and if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the canonical factorization of $n$, then all positive divisors of $n$ are of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ where $0 \le b_i \le a_i$ for every $i$. In this case, by a simple counting argument, we see that

$$d(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1).$$

From this, it is easy to see that $d$ is a multiplicative function. We record the above discussion in the next theorem.

**Theorem 2.8.** *The functions $e$, $1$, $N$, and $\lambda$ are completely multiplicative. The divisor function $d$ is multiplicative and satisfies $d(n) = \prod_{p^k \| n}(k+1)$. The Möbius function $\mu$ is multiplicative.*

**Proof.** As already discussed above, it remains to show that $\mu$ is multiplicative. Assume that $m, n \in \mathbb{N}$ and $(m, n) = 1$. We need to check the validity of the following equation:

$$\mu(mn) = \mu(m)\mu(n). \tag{2.3}$$

If $m = 1$ or $n = 1$, then (2.3) obviously holds. So we assume that $m > 1$ and $n > 1$. If $m$ or $n$ are not squarefree, then $mn$ is not squarefree and both sides of (2.3) are zero. If $m$ and $n$ are squarefree, then we can write $m = p_1 p_2 \cdots p_k$ and $n = q_1 q_2 \cdots q_\ell$ where $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_\ell$ are distinct primes, and thus

$$\begin{aligned} \mu(mn) &= \mu(p_1 p_2 \cdots p_k q_1 q_2 \cdots q_\ell) \\ &= (-1)^{k+\ell} = (-1)^k (-1)^\ell = \mu(m)\mu(n). \end{aligned}$$

So (2.3) holds for every $m, n \in \mathbb{N}$ with $(m, n) = 1$, as required. □

The functions $\varphi$ and $\sigma$ are also multiplicative but this is less obvious. We postpone the proof to the next section.

## 2.3. Dirichlet Product

The sum of the following form occurs frequently in number theory:

$$\sum_{d \mid n} f(d), \text{ or more generally, } \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right)$$

where $f$ and $g$ are arithmetic functions, and $d$ runs over all positive divisors of $n$. The first sum is usually called a *divisor sum of $f$*. For the second sum, it is useful to view it as a new kind of multiplication $*$ between $f$ and $g$. Algebraic properties of $*$ show that $(\mathcal{M}, *)$ is an abelian group. By connecting this to a concept of group theory, the calculations in the next section seem natural and follow the same pattern as those we learn in a first course in abstract algebra. The definition of the Dirichlet multiplication $*$ is as follows.

**Definition 2.9.** Let $f$ and $g$ be arithmetic functions. The *Dirichlet product* (or *Dirichlet convolution*, or *Dirichlet multiplication*) of $f$ and $g$, denoted by $f * g$, is defined for every $n \in \mathbb{N}$ by

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

For example, by the above definition, we have,

$$\begin{aligned}(f * g)(10) &= f(1)g(10) + f(2)g(5) + f(5)g(2) + f(1)g(10)\\ &= \sum_{ab=10} f(a)g(b),\end{aligned}$$

where $a$ and $b$ run over the positive integers satisfying $ab = 10$. In general, $(f * g)(n)$ can also be written as $\sum_{ab=n} f(a)g(b)$. This will be used in the proof of the following theorem.

**Theorem 2.10.** *Let $f$ and $g$ be arithmetic functions. Then the following statements hold.*

(i) $f * g = g * f$.

(ii) $(f * g) * h = f * (g * h)$.

(iii) $e * f = f * e = f$.

*That is, the Dirichlet multiplication is commutative, associative, and has $e$ as the identity.*

**Proof.** Let $n \in \mathbb{N}$. As discussed above,

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{ba=n} g(b)f(a) = (g * f)(n), \text{ and}$$

$$\begin{aligned}((f * g) * h)(n) &= \sum_{ab=n} (f * g)(a)h(b) = \sum_{ab=n} \sum_{cd=a} f(c)g(d)h(b)\\ &= \sum_{cdb=n} f(c)g(d)h(b) = \sum_{\ell km=n} f(\ell)g(k)h(m).\end{aligned}$$

On the other hand, $(f * (g * h))(n)$ is

$$\begin{aligned}\sum_{ab=n} f(a)(g*h)(b) &= \sum_{ab=n}\sum_{cd=b} f(a)g(c)h(d) = \sum_{acd=n} f(a)g(c)h(d)\\ &= \sum_{\ell km=n} f(\ell)g(k)h(m),\end{aligned}$$

which is the same as $((f * g) * h)(n)$. For (iii), $(e * f)(n)$ is

$$\sum_{ab=n} e(a)f(b) = e(1)f(n) + \sum_{\substack{ab=n\\ a>1}} e(a)f(n) = f(n) + 0 = f(n).$$

Similarly, $(f*e)(n) = f(n)$. This proves (iii) and so the proof is complete. □

**Theorem 2.11.** *Let $f$ be an arithmetic function and let $f(1) \neq 0$. Then there exists a unique arithmetic function $g$ satisfying $g * f = f * g = e$. Moreover, $g$ can be given explicitly by the recurrence relation:*

$$g(1) = \frac{1}{f(1)}, \text{ and } g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n\\ d<n}} g(d)f\left(\frac{n}{d}\right) \text{ for } n > 1.$$

(*The function $g$ is called the Dirichlet inverse of $f$ and is denoted by $f^{-1}$.*)

**Proof.** We will show that the equation

$$(g * f)(n) = e(n) \tag{2.4}$$

has a unique solution $g$. If $n = 1$, then (2.4) becomes $g(1)f(1) = 1$. So $g(1) = \frac{1}{f(1)}$. Let $n \geq 2$ and assume that the values $g(1), g(2), \ldots, g(n-1)$ are already defined. Then (2.4) implies that

$$0 = e(n) = \sum_{d|n} g(d)f\left(\frac{n}{d}\right) = g(n)f(1) + \sum_{\substack{d|n\\ d<n}} g(d)f\left(\frac{n}{d}\right).$$

Therefore

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n\\ d<n}} g(d)f\left(\frac{n}{d}\right).$$

Since $g(d)$ are defined for all $d < n$, the above gives a unique value of $g(n)$. This establishes the existence and uniqueness of $g$ by induction. □

Let $\mathcal{A}$ be the set of all arithmetic functions and let $\mathcal{A}^{\times}$ be the set of all $f \in \mathcal{A}$ with $f(1) \neq 0$. If $f, g \in \mathcal{A}^{\times}$, then

$$(f * g)(1) = f(1)g(1) \neq 0,$$

and thus $f * g \in \mathcal{A}^{\times}$. Therefore $*$ is a binary operation on $\mathcal{A}^{\times}$ and we have the following result.

**Corollary 2.12.** *$(\mathcal{A}^{\times}, *)$ is an abelian group.*

**Proof.** This follows from Theorems 2.10 and 2.11, and the above discussion. ☐

Next we show that $(\mathcal{M}, *)$ is also an abelian group. Since $\mathcal{M}$ is a subset of $\mathcal{A}^{\times}$, it suffices to show that $(\mathcal{M}, *)$ is a subgroup of $(\mathcal{A}^{\times}, *)$. Therefore we only need to show that if $f, g \in \mathcal{M}$, then $f * g$ and $f^{-1}$ are also in $\mathcal{M}$. The proof of this is divided into three parts as shown in the next three theorems.

**Theorem 2.13.** *If $f$ and $g$ are multiplicative, then $f * g$ is also multiplicative.*

**Proof.** Let $m, n \in \mathbb{N}$ with $(m, n) = 1$. Each divisor $d$ of $mn$ can be expressed as $d = ab$ where $a \mid m$ and $b \mid n$. In addition, $(a, b) = 1$, $\left(\frac{m}{a}, \frac{n}{b}\right) = 1$, and there is a one-to-one correspondence between the set of products $ab$ and the divisors $d$ of $mn$. Therefore

$$\begin{aligned}(f * g)(mn) &= \sum_{d \mid mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{\substack{a \mid m \\ b \mid n}} f(ab)g\left(\frac{mn}{ab}\right) \\ &= \sum_{\substack{a \mid m \\ b \mid n}} f(a)g\left(\frac{m}{a}\right) f(b)g\left(\frac{n}{b}\right) = \sum_{a \mid m} f(a)g\left(\frac{m}{a}\right) \sum_{b \mid n} f(b)g\left(\frac{n}{b}\right) \\ &= (f * g)(m)(f * g)(n).\end{aligned}$$

Hence $f * g$ is multiplicative. ☐

**Theorem 2.14.** *If $g$ and $f * g$ are multiplicative, then $f$ is also multiplicative.*

**Proof.** Suppose for a contradiction that $g$ and $f * g$ are multiplicative but $f$ is not multiplicative. Then there exist $m, n \in \mathbb{N}$ such that $(m, n) = 1$ and

$$f(mn) \neq f(m)f(n). \tag{2.5}$$

We can choose the pair $m$, $n$ so that the product $mn$ is minimal. If $mn = 1$, then (2.5) becomes $f(1) \neq f(1)f(1)$ and by the assumption that $f * g$ and $g$ are multiplicative, we obtain

$$1 = (f * g)(1) = f(1)g(1) = f(1),$$

which contradicts $f(1) \neq f(1)f(1)$. Therefore $mn > 1$. Then $f(ab) = f(a)f(b)$ for all positive integers $a$, $b$ with $(a, b) = 1$ and $ab < mn$. Applying the same idea from the proof of Theorem 2.13, we obtain that $(f * g)(mn)$ is equal to

$$\begin{aligned}
\sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) &= \sum_{\substack{a|m, b|n, \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) \\
&= \sum_{\substack{a|m, b|n, \\ ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) + f(mn) \\
&= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) - f(m)f(n) + f(mn) \\
&= (f * g)(m)(f * g)(n) - f(m)f(n) + f(mn) \\
&= (f * g)(mn) - f(m)f(n) + f(mn),
\end{aligned}$$

where we use the assumption that $f * g$ is multiplicative. The above implies that $f(mn) = f(m)f(n)$, which contradicts (2.5). So the proof is complete. □

**Theorem 2.15.** *If $f$ is multiplicative, then so is $f^{-1}$.*

**Proof.** If $f$ is multiplicative, then $f$ and $f^{-1} * f$ are multiplicative and we obtain by Theorem 2.14 that $f^{-1}$ is also multiplicative. □

**Corollary 2.16.** *$(\mathcal{M}, *)$ is an abelian group.*

**Proof.** Since $f(1) = 1 \neq 0$ for every $f \in \mathcal{M}$, we see that $\mathcal{M} \subseteq \mathcal{A}^{\times}$. By Theorem 2.13 and Theorem 2.15, we see that $(\mathcal{M}, *)$ is a subgroup of $(\mathcal{A}^{\times}, *)$. By Corollary 2.12, we obtain the desired result. □

## 2.4. Divisor Sums and the Möbius Inversion Formula

The sum of the form $\sum_{d|n} f(d)$ can be viewed as $(f * 1)(n)$. The next theorem simply says that $\mu$ and 1 are Dirichlet inverse of each other.

For some generalizations, see Section 2.5 and Exercises 2.6.6, 2.6.7, and 2.6.22.

**Theorem 2.17.** *For every $n \geq 1$, we have*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n > 1. \end{cases}$$

*In other words, $\mu * 1 = e$.*

**Proof.** The case $n = 1$ is obvious. So assume that $n > 1$ and write $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ in the canonical factorization. Consider $\sum_{d|n} \mu(d)$. Since $\mu(d) = 0$ if $d$ is not squarefree, we see that $\mu(d) \neq 0$ only when $d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ where $b_i \in \{0, 1\}$ for every $i$. So the sum in question is equal to

$$\begin{aligned} \sum_{d|p_1 p_2 \cdots p_k} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) \\ &\quad + \sum_{1 \leq i < j \leq k} \mu(p_i p_j) + \cdots + \mu(p_1 p_2 \cdots p_k) \\ &= 1 + (-1)^1 \binom{k}{1} + (-1)^2 \binom{k}{2} + \cdots + (-1)^k. \end{aligned} \tag{2.6}$$

By the binomial theorem, $(1 + x)^k = 1 + \binom{k}{1}x + \binom{k}{2}x^2 + \cdots + \binom{k}{k}x^k$. Substituting $x = -1$, we see that (2.6) is equal to zero. This completes the proof.

**Alternative proof.** Since $\mu$ and 1 are multiplicative, we obtain that $\mu * 1$ is multiplicative. In addition,

$$(\mu * 1)(p^a) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^a) = 0 = e(p^a).$$

Therefore we obtain by Corollary 2.7 that $\mu * 1 = e$. □

The fact that $\mu * 1 = e$ leads to a simple proof of the next theorem.

**Theorem 2.18.** (Möbius Inversion Formula) *Suppose that $f$ and $g$ are arithmetic functions. Then $f = g * 1$ if and only if $g = \mu * f$. In other words,*

$$f(n) = \sum_{d|n} g(d) \text{ for every } n \geq 1$$

*if and only if*

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \text{ for every } n \geq 1.$$

**Proof.** If $f = g*1$, then $\mu*f = f*\mu = (g*1)*\mu = g*(1*\mu) = g*(\mu*1) = g*e = g$. Conversely, if $g = \mu * f$, then $g*1 = (1*\mu)*f = e*f = f$. ☐

We consider the divisor sum of Liouville's and Euler's functions in the next two theorems.

**Theorem 2.19.** *For every $n \geq 1$,*

$$\sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{if } n \text{ is a square;} \\ 0, & \text{otherwise.} \end{cases}$$

**Proof.** The proof is similar to that of Theorem 2.17. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $a_1, a_2, \ldots, a_k$ are nonnegative integers. The divisors of $n$ are of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ where $0 \leq b_i \leq a_i$ for every $i$. Then

$$\begin{aligned} \sum_{d|n} \lambda(d) &= \sum_{\substack{0 \leq b_i \leq a_i \\ \text{for every } i}} \lambda\left(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}\right) \\ &= \sum_{0 \leq b_1 \leq a_1, 0 \leq b_2 \leq a_2, \ldots, 0 \leq b_k \leq a_k} (-1)^{b_1 + b_2 + \cdots + b_k} \\ &= \left(\sum_{0 \leq b_1 \leq a_1} (-1)^{b_1}\right)\left(\sum_{0 \leq b_2 \leq a_2} (-1)^{b_2}\right) \cdots \left(\sum_{0 \leq b_k \leq a_k} (-1)^{b_k}\right). \qquad (2.7) \end{aligned}$$

It is easy to see that $\sum_{0 \leq b \leq a} (-1)^b$ is equal to 1 if $a$ is even, and is equal to 0 if $a$ is odd. Therefore (2.7) is equal to 1 if all $a_i$ are even and is equal to 0 otherwise. This implies the desired result. ☐

**Theorem 2.20.** *We have $\varphi * 1 = N$. That is*

$$\sum_{d|n} \varphi(d) = n \quad \text{for every } n \in \mathbb{N}.$$

**Proof.** Let $S = \{1, 2, 3, \ldots, n\}$. For each $d \mid n$, let

$$A(d) = \{k \in S \mid (k, n) = d\}.$$

Then it is easy to check that the sets $A(d)$ form a partition of $S$. That is, each distinct $A(d)$ is nonempty and disjoint and $\bigcup_{d|n} A(d) = S$. Therefore

$$n = |S| = \sum_{d|n} |A(d)|. \tag{2.8}$$

We view $A(d)$ as the set $\left\{k \;:\; d \mid k, 1 \le \frac{k}{d} \le \frac{n}{d} \text{ and } \left(\frac{k}{d}, \frac{n}{d}\right) = 1\right\}$, which has a one-to-one correspondence with the set

$$\left\{\ell \mid 1 \le \ell \le \frac{n}{d} \text{ and } \left(\ell, \frac{n}{d}\right) = 1\right\}.$$

So $|A(d)| = \varphi\left(\frac{n}{d}\right)$ and (2.8) becomes

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

As $d$ runs through the divisors of $n$, so is $\frac{n}{d}$. Hence the above is also equal to $\sum_{d|n} \varphi(d)$, as required. This idea is used often in certain situations and it can be written in a shorter form as follows.

**Another form of the proof.** We have

$$\begin{aligned} n &= \sum_{1\le k\le n} 1 = \sum_{d|n} \sum_{\substack{1\le k\le n\\(k,n)=d}} 1 = \sum_{d|n} \sum_{\substack{1\le \frac{k}{d}\le \frac{n}{d}\\ \left(\frac{k}{d},\frac{n}{d}\right)=1}} 1 \\ &= \sum_{d|n} \sum_{\substack{1\le \ell\le \frac{n}{d}\\ \left(\ell,\frac{n}{d}\right)=1}} 1 = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d). \end{aligned}$$

☐

By the above idea, we obtain the following observation.

**Theorem 2.21.** *For any function $F : [0,1] \to \mathbb{C}$, we have*

$$\sum_{1\le k\le n} F\left(\frac{k}{n}\right) = \sum_{d|n} \sum_{\substack{1\le k\le n\\(k,n)=d}} F\left(\frac{k}{n}\right) = \sum_{d|n} \sum_{\substack{1\le a\le d\\(a,d)=1}} F\left(\frac{a}{d}\right).$$

**Proof.** This follows from the same idea used in the proof of Theorem 2.20. The details are left to the reader. See also Exercises 2.6.17 to 2.6.19 for similar problems. ☐

The next result is also useful in evaluating certain divisor sums.

**Theorem 2.22.** *Let $f$ be a multiplicative function. Then for every $n \in \mathbb{N}$, we have*

$$\sum_{d|n} f(d) = \prod_{p^a \| n} \left(1 + f(p) + f(p^2) + \cdots + f(p^a)\right). \tag{2.9}$$

**Proof.** If $n = 1$, then both sides are equal to 1. So assume that $n > 1$ and write $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ in the canonical factorization. The summands in the left-hand side of (2.9) are of the form

$$f(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}) = f(p_1^{b_1}) f(p_2^{b_2}) \cdots f(p_k^{b_k})$$

where $0 \leq b_i \leq a_i$ for each $i$. On the other hand, after we multiply every factor, each term on the right-hand side of (2.9) is of the form $f(p_1^{b_1}) f(p_2^{b_2}) \cdots f(p_k^{b_k})$ where $0 \leq b_i \leq a_i$ for every $i$. Hence (2.9) holds. □

The remaining theorems or examples in this section are well known and we record them for completeness. It is also useful to try applying our previous idea and results in the proof of the following theorems and examples.

**Theorem 2.23.** *Let $n \in \mathbb{N}$. Then the following statements hold.*

(i) $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.

(ii) *$\varphi$ is multiplicative.*

(iii) $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

**Proof.** Since $\varphi * 1 = N$, we obtain by the Möbius inversion formula that $\varphi = N * \mu$, which implies (i). Since $N$ and $\mu$ are multiplicative, (ii) follows. For (iii), we apply (i) and Theorem 2.22 to obtain

$$\begin{aligned} \varphi(n) &= n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p^a \| n} \left(1 + \frac{\mu(p)}{p} + \frac{\mu(p^2)}{p^2} + \cdots + \frac{\mu(p^a)}{p^a}\right) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right). \end{aligned}$$

□

**Example 2.24.** Show that for every $n \in \mathbb{N}$,

$$\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}.$$

**Solution.** Since $\frac{\mu^2}{\varphi}$ is multiplicative and $\mu^2(p^a) = 0$ if $a \geq 2$, we obtain by Theorems 2.22 and 2.23 that the sum in question is equal to

$$\prod_{p|n}\left(1 + \frac{\mu^2(p)}{\varphi(p)}\right) = \prod_{p|n}\left(1 + \frac{1}{p-1}\right) = \frac{n}{\varphi(n)}.$$

*Alternative Solution.* Both sides of the equation are multiplicative, so if they agree at the prime powers they agree everywhere. If $n = p^a$ it is easy to check that each side is equal to $\frac{p}{p-1}$. ☐

**Remark 2.25.** There are many ways to obtain the properties of $\varphi$ given in Theorem 2.23. For example, we can apply the results on the residue classes and the inclusion-exclusion principle to obtain Theorem 2.23(iii) and then use (iii) to obtain (ii). We can also obtain (i) from (iii) and Theorem 2.22. We give some details in the next example.

**Example 2.26.** The inclusion-exclusion principle states that if $A_1, A_2, \ldots, A_n$ are finite sets, then

$$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1\leq i_1<i_2\leq n} |A_{i_1} \cap A_{i_2}| \\ + \sum_{1\leq i_1<i_2<i_3\leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \cdots \\ + (-1)^{n+1}|A_1 \cap A_2 \cap \cdots A_n|.\end{aligned}$$

Use this to give another proof of the formula $\varphi(n) = n\prod_{p|n}(1 - 1/p)$. Hint: For each $p \mid n$, let $A_p$ be the set of positive integers $m$ such that $1 \leq m \leq n$ and $p \mid m$. Then show that $\varphi(n) = n - \left|\bigcup_{p|n} A_p\right|$.

**Solution.** For $1 \leq m \leq n$, we have $(m, n) > 1$ if and only if $m \in A_p$ for some $p \mid n$. Therefore $\varphi(n) = n - \left|\bigcup_{p|n} A_p\right|$. By the inclusion-exclusion principle, $\left|\bigcup_{p|n} A_p\right|$ is equal to

$$\sum_{p|n} |A_p| - \sum_{\substack{p_1,p_2|n \\ p_1<p_2}} |A_{p_1} \cap A_{p_2}| + \cdots = \sum_{p|n} \frac{n}{p} - \sum_{\substack{p_1,p_2|n \\ p_1<p_2}} \frac{n}{p_1p_2} + \cdots.$$

Therefore $\varphi(n)$ is equal to

$$n\left(1 - \sum_{p|n}\frac{1}{p} + \sum_{\substack{p_1,p_2|n \\ p_1<p_2}} \frac{1}{p_1p_2} - \cdots\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right).$$ ☐

**Theorem 2.27.** *The following statements hold.*

(i) $\varphi(p^a) = p^a - p^{a-1}$ *for a prime* $p$ *and* $a \geq 1$.

(ii) $\varphi(mn) = \varphi(m)\varphi(n)(d/\varphi(d))$ *where* $d = (m, n)$.

**Proof.** The proof can be obtained by applying Theorem 2.23 and is left as an exercise for the reader. ☐

We can now give another proof of the results on the multiplicative property of the functions given in Section 1. For example, since $\sigma = N{*}1$, $\sigma$ is multiplicative. In addition, $d = 1 * 1$, so $d$ is multiplicative, and since $\mu$ is the inverse of 1, $\mu$ is also multiplicative. We record the results concerning the multiplicative property in the next theorem.

**Theorem 2.28.** *The functions* $e$, $1$, $N$, $\lambda$ *are completely multiplicative. The functions* $d$, $\mu$, $\varphi$, *and* $\sigma$ *are multiplicative.*

**Theorem 2.29.** *We have* $\sigma(p^a) = (p^{a+1} - 1)/(p-1)$ *for each prime* $p$ *and positive integer* $a$ *and if* $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ *is the canonical factorization of* $n$ *then*

$$\sigma(n) = \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{a_2+1} - 1}{p_2 - 1}\right)\cdots\left(\frac{p_k^{a_k+1} - 1}{p_k - 1}\right).$$

**Proof.** Since the positive divisors of $p^a$ are $1, p, p^2, \ldots, p^a$, which is a geometric progression, so the sum $\sigma(p^a)$ can be obtained from the well-known formula. This proves the first part. The second part follows from the first and the multiplicative property of $\sigma$. ☐

One can extend the above idea to obtain the formula for $\sigma_k(n)$, that is, $\sigma_k$ is multiplicative and $\sigma_k(p^a) = \frac{p^{k(a+1)}-1}{p^k-1}$. Exercises 2.6.24 and 2.6.25 give more details about this extension.

Next, we give easy but important results on the divisor sum of the von Mangoldt function in the following two theorems.

**Theorem 2.30.** *We have* $\Lambda * 1 = \log$. *In other words,*

$$\sum_{d|n} \Lambda(d) = \log n \quad \textit{for every } n \in \mathbb{N}.$$

**Proof.** If $n = 1$, then both sides are zero. So let $n > 1$ and write $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ in the canonical form. Since $\Lambda(d) = 0$ if $d$ is not a power of primes, we obtain that

$$\begin{aligned}\sum_{d|n} \Lambda(d) &= \sum_{m=1}^{a_1} \Lambda(p_1^m) + \sum_{m=1}^{a_2} \Lambda(p_2^m) + \cdots + \sum_{m=1}^{a_k} \Lambda(p_k^m) \\ &= a_1 \log p_1 + a_2 \log p_2 + \cdots + a_k \log p_k \\ &= \log\left(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\right) = \log n. \end{aligned}$$ □

**Theorem 2.31.** *For $n \geq 1$, we have*

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d.$$

**Proof.** By Theorem 2.30 and the Möbius inversion formula, we see that

$$\begin{aligned}\Lambda(n) &= \sum_{d|n} \mu(d) \log \frac{n}{d} = (\log n) \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= -\sum_{d|n} \mu(d) \log d.\end{aligned}$$ □

## 2.5. Extensions of the Möbius Inversion Formula

Throughout this section, we let $F, G : (0, \infty) \to \mathbb{C}$ satisfy

$$F(x) = G(x) = 0 \quad \text{for } x \in (0, 1),$$

and let $\alpha$ be an arithmetic function. Another form of sums which arise frequently in number theory is

$$\sum_{n \leq x} F\left(\frac{x}{n}\right), \text{ or more generally, } \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

If $x \in \mathbb{N}$ and $F(y) = 0$ for all $y \notin \mathbb{Z}$, then the above sum is the Dirichlet product of $\alpha$ and $F\ |_{\mathbb{N}}$. The following two theorems give an inversion formula for this type of sum.

**Theorem 2.32.** *Suppose that $\alpha$ has a Dirichlet inverse $\alpha^{-1}$. Then*

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \text{ for all } x \in (0, \infty) \tag{2.10}$$

*if and only if*

$$F(x) = \sum_{n \leq x} \alpha^{-1}(n) G\left(\frac{x}{n}\right) \text{ for all } x \in (0, \infty). \tag{2.11}$$

**Proof.** Suppose (2.10) holds. Then the right-hand side of (2.11) is

$$\sum_{n\le x}\alpha^{-1}(n)\sum_{m\le\frac{x}{n}}\alpha(m)F\left(\frac{x}{nm}\right)=\sum_{mn\le x}\alpha^{-1}(n)\alpha(m)F\left(\frac{x}{nm}\right)$$
$$=\sum_{k\le x}F\left(\frac{x}{k}\right)\sum_{mn=k}\alpha^{-1}(n)\alpha(m)=\sum_{k\le x}F\left(\frac{x}{k}\right)(\alpha^{-1}*\alpha)(k)=F(x).$$

The converse is similar. ☐

**Corollary 2.33.** *We have*

$$G(x)=\sum_{n\le x}F\left(\frac{x}{n}\right)\text{ for all }x\in(0,\infty)\text{ if and only if}$$
$$F(x)=\sum_{n\le x}\mu(n)G\left(\frac{x}{n}\right)\text{ for all }x\in(0,\infty).$$

**Proof.** In this case, $\alpha=1$ and $\alpha^{-1}=\mu$. (See also Exercise 2.6.22). ☐

There are other forms of the Möbius inversion formulas too. For example, Theorem 2.34 is a version that involves infinite series as shown below.

**Theorem 2.34.** *Suppose that the series*

$$\sum_{m,n=1}^{\infty}\mu(n)F(mnx)\quad\text{and}\quad\sum_{m,n=1}^{\infty}\mu(n)G(mnx)$$

*converge absolutely for all* $x\in(0,\infty)$. *Then*

$$G(x)=\sum_{m=1}^{\infty}F(mx)\text{ for all }x\in(0,\infty)\tag{2.12}$$

*if and only if*

$$F(x)=\sum_{n=1}^{\infty}\mu(n)G(nx)\text{ for all }x\in(0,\infty).\tag{2.13}$$

**Proof.** Suppose (2.12) holds. Then the right-hand side of (2.13) is

$$\sum_{n=1}^{\infty}\mu(n)\sum_{m=1}^{\infty}F(mnx)=\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\mu(n)F(mnx).$$

Since $\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}|\mu(n)F(mnx)|$ converges, we can rearrange the above sum as

$$\sum_{k=1}^{\infty} F(kx) \sum_{nm=k} \mu(n) = \sum_{k=1}^{\infty} F(kx) \sum_{n|k} \mu(n) = F(x).$$

The converse is similar. □

Another version of the Möbius inversion formula is as follows.

**Theorem 2.35.** (Product form of the Möbius Inversion Formula) *Suppose $f(n) > 0$, $g(n) > 0$, $a(1) \neq 0$, and $a(n)$ is real for all $n \in \mathbb{N}$. Then*

$$g(n) = \prod_{d|n} f(d)^{a(n/d)} \quad \textit{for all } n \textit{ if and only if}$$
$$f(n) = \prod_{d|n} g(d)^{b(n/d)} \textit{for all } n,$$

*where $b = a^{-1}$, the Dirichlet inverse of $a$.*

**Proof.** Because $g(n)$ is positive, we can take logarithms, and the formula for $g(n)$ becomes

$$\log g(n) = \sum_{d|n} a(n/d) \log f(d) \quad \text{for all } n.$$

We then invert this to obtain

$$\log f(n) = \sum_{d|n} b(n/d) \log g(n) \quad \text{for all } n.$$

Exponentiating this, we get the formula for $f(n)$. These steps are reversible, so the converse also holds.

*Alternative proof.* We can also calculate this directly as in the proof of the Möbius inversion formula. The calculation is a bit longer but is a good exercise. We show the direct part and leave the converse to the reader. We have

$$\begin{aligned}\prod_{d|n} g(d)^{b\left(\frac{n}{d}\right)} &= \prod_{d|n}\left(\prod_{\ell|d} f(\ell)^{a\left(\frac{d}{\ell}\right)}\right)^{b\left(\frac{n}{d}\right)} = \prod_{d|n}\prod_{\ell|d} f(\ell)^{a\left(\frac{d}{\ell}\right)b\left(\frac{n}{d}\right)} \\ &= \prod_{\ell|n}\prod_{\substack{d|n \\ \ell|d}} f(\ell)^{a\left(\frac{d}{\ell}\right)b\left(\frac{n}{d}\right)} = \prod_{\ell|n} f(\ell)^{A(n,\ell)},\end{aligned}$$

where

$$A(n,\ell) = \sum_{\substack{d|n \\ \ell|d}} a\left(d/\ell\right) b\left(n/d\right) = \sum_{q|\frac{n}{\ell}} a(q) b\left(\frac{n}{\ell q}\right) = (a * b)\left(\frac{n}{\ell}\right),$$

which is equal to 1 if $\ell = n$ and is zero otherwise. This implies the desired result. ☐

Theorem 2.35 and the idea in the proof of Theorem 2.21 can be used to obtain a formula for the product of all positive integers that are coprime to $n$ as shown in the next example.

**Example 2.36.** For each $n \in \mathbb{N}$, let $P(n)$ be the product of the positive integers which are less than or equal to $n$ and relatively prime to $n$. Prove that

$$P(n) = n^{\varphi(n)} \prod_{d|n} \left(\frac{d!}{d^d}\right)^{\mu(n/d)}.$$

**Solution.** We write $n!$ as

$$\begin{aligned}\prod_{k=1}^{n} k = \prod_{d|n} \prod_{\substack{k=1 \\ (k,n)=d}}^{n} k = \prod_{d|n} \prod_{\substack{\ell=1 \\ (\ell,\frac{n}{d})=1}}^{\frac{n}{d}} d\ell = \prod_{d|n} d^{\varphi(\frac{n}{d})} P\left(\frac{n}{d}\right) \\ = \left(\prod_{d|n} \left(\frac{n}{d}\right)^{\varphi(d)} P(d)\right) = \left(n^{\sum_{d|n}\varphi(d)}\right)\left(\prod_{d|n} \frac{P(d)}{d^{\varphi(d)}}\right) \\ = n^n \left(\prod_{d|n} \frac{P(d)}{d^{\varphi(d)}}\right).\end{aligned}$$

Therefore $\frac{n!}{n^n} = \prod_{d|n} \frac{P(d)}{d^{\varphi(d)}}$ for all $n \in \mathbb{N}$. By Theorem 2.35, we obtain $\frac{P(n)}{n^{\varphi(n)}} = \prod_{d|n} \left(\frac{d!}{d^d}\right)^{\mu(\frac{n}{d})}$ for all $n \in \mathbb{N}$, which leads to the desired formula. We can also compute $P(n)$ without using Theorem 2.35. We leave this as an exercise to the reader (see Exercise 2.6.16). ☐

## 2.6. Exercises

2.6.1 Show that $\Omega$ is completely additive, $\omega$ is strongly additive, and $\Lambda$ is not additive. (Their definitions are given in Section 2.1.)

2.6.2 Let $f, g : \mathbb{N} \to \mathbb{R}$, $f(n) > 0$ and $g(n) = \log f(n)$ for all $n \in \mathbb{N}$. Show that

(i) if $f$ is multiplicative, then $g$ is additive,
(ii) if $f$ is completely multiplicative, then $g$ is completely additive,
(iii) if $f$ is strongly multiplicative, then $g$ is strongly additive.

2.6.3 Let $\gamma(1) = 1$ and $\gamma(n) = \prod_{p|n} p$ for each $n > 1$. Show that

$$\sum_{k|n} d(k) = \frac{d(n)d(n\gamma(n))}{2^{\omega(n)}}.$$

2.6.4 Show that for every $n \geq 1$, $\sum\limits_{d|n} |\mu(d)| = 2^{\omega(n)}$.

2.6.5 If $f = \mu * \omega$, prove that for each $n \in \mathbb{N}$, $f(n)$ is either 0 or 1. Similarly, show that if $f = \mu * \Omega$, then $f(n) \in \{0, 1\}$ for all $n \in \mathbb{N}$.

2.6.6 Let $k$ be a positive integer. Prove that

$$\sum_{d^k|n} \mu(d) = \begin{cases} 0, & \text{if } b^k \mid n \text{ for some } b > 1; \\ 1, & \text{otherwise.} \end{cases}$$

Here the sum is extended over all positive divisors $d$ of $n$ such that $d^k \mid n$.

2.6.7 Prove that for each prime $p$, we have

$$\sum_{d|n} \mu(d)\mu(\gcd(p, d)) = \begin{cases} 1, & \text{if } n = 1; \\ 2, & \text{if } n = p^a \text{ for some } a \geq 1; \\ 0, & \text{otherwise.} \end{cases}$$

2.6.8 For each $n \in \mathbb{N}$, let $a(n)$ be the number of primes $p$ such that $p \parallel n$. Show that

$$\sum_{d|n} \mu(d)\mu\left(\frac{n}{d}\right) = \begin{cases} 0, & \text{if } p^3 \mid n \text{ for some prime } p; \\ (-2)^{a(n)}, & \text{otherwise.} \end{cases}$$

2.6.9 Let $\mu^{(1)} = \mu$ be the Möbius function and let

$$\mu^{(m)} = \mu^{(m-1)} * \mu \quad \text{for each } m \geq 2.$$

In addition, for each $k, n \in \mathbb{N}$, let $a_k(n) = \sum_{p^k \| n} 1$ be the number of primes $p$ such that $p^k \| n$. Show that

$$\mu^{(m)}(n) = \begin{cases} 0, & \text{if } p^{m+1} \mid n \\ & \text{for some prime } p; \\ \displaystyle\prod_{k=1}^{n} \left((-1)^k \binom{m}{k}\right)^{a_k(n)}, & \text{otherwise,} \end{cases}$$

where $\binom{m}{k}$ is the binomial coefficient.

2.6.10 Prove that $\varphi(n) > n/6$ for all $n$ with at most eight distinct prime factors.

2.6.11 Prove that $d(n)$ is odd if and only if $n$ is a square.

2.6.12 Prove that $\displaystyle\prod_{t|n} t = n^{d(n)/2}$.

2.6.13 Prove that $\displaystyle\sum_{t|n} d(t)^3 = \left(\sum_{t|n} d(t)\right)^2$.

2.6.14 For each real number $x \geq 1$, let $\varphi(x, n)$ denote the number of positive integers $\leq x$ that are relatively prime to $n$. Prove that

$$\varphi(x, n) = \sum_{d|n} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor \quad \text{and} \quad \sum_{d|n} \varphi\left(\frac{x}{d}, \frac{n}{d}\right) = \lfloor x \rfloor .$$

2.6.15 Let $\tau(n)$ be the number of positive divisors of $n$. Prove that the following equalities hold for all $n \in \mathbb{N}$.

(i) $\displaystyle\sum_{d|n} \sigma(d) = n \sum_{d|n} \frac{\tau(d)}{d}$.

(ii) $\displaystyle\sum_{d|n} \varphi(d)\tau\left(\frac{n}{d}\right) = \sigma(n)$.

(iii) $\displaystyle\sum_{d|n} \varphi(d)\sigma\left(\frac{n}{d}\right) = n\tau(n)$.

(iv) $\displaystyle\sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\tau(d)$.

(v) $\displaystyle\sum_{m|n} md(m) = \sum_{m|n} \left(\frac{n}{m}\right)\sigma(m)$

(vi) $\displaystyle\sum_{d|n} \sigma(d)\sigma\left(\frac{n}{d}\right) = \sum_{d|n} d\tau(d)\tau\left(\frac{n}{d}\right)$.

2.6.16 Let $P(n)$ be as in Example 2.36. Compute $P(n)$ without using Theorem 2.35.

2.6.17 Let $f(x)$ be defined for all rational $x$ in $[0,1]$ and let

$$F(n) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right) \quad \text{and} \quad F_1(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} f\left(\frac{k}{n}\right).$$

(i) Show that $F_1 = \mu * F$.

(ii) Prove that $\mu(n)$ is the sum of the primitive $n$th roots of unity:

$$\mu(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} e^{2\pi ik/n}.$$

2.6.18 Let $\varphi_k(n)$ denote the sum of the $k$th powers of the integers that are at most $n$ and relatively prime to $n$. We note that $\varphi_0(n) = \varphi(n)$. Use Exercise 2.6.17 or some other means to prove that

$$\sum_{d|n} \frac{\varphi_k(d)}{d^k} = \frac{1^k + \cdots + n^k}{n^k}.$$

2.6.19 Invert the formula in Exercise 2.6.18 to obtain, for $n > 1$,

$$\varphi_1(n) = \frac{1}{2}n\varphi(n), \quad \varphi_2(n) = \frac{1}{3}n^2\varphi(n) + \frac{n}{6}\prod_{p|n}(1-p), \quad \text{and}$$

$$\varphi_3(n) = \frac{1}{4}n^3\varphi(n) + \frac{n^2}{4}\prod_{p|n}(1-p).$$

2.6.20 Suppose that $f$ is completely multiplicative and $f^{-1}$ is the Dirichlet inverse of $f$. Show that $f^{-1}(n) = \mu(n)f(n)$ for all $n \geq 1$.

2.6.21 Prove that there is a multiplicative function $g$ such that

$$\sum_{k=1}^{n} f((k,n)) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

for every arithmetic function $f$. Here $(k,n)$ is the gcd of $n$ and $k$. Use this identity to prove that

$$\sum_{k=1}^{n} (k,n)\mu\left((k,n)\right) = \mu(n).$$

2.6.22 Let $F, G : (0,\infty) \to \mathbb{R}$ and $\alpha$ be a completely multiplicative function. Show that

$$G(x) = \sum_{n \le x} \alpha(n) F\left(\frac{x}{n}\right) \text{ for all } x \in (0,\infty) \text{ if and only if}$$

$$F(x) = \sum_{n \le x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right) \text{ for all } x \in (0,\infty).$$

2.6.23 Let $\varphi^{-1}$ and $\lambda^{-1}$ be the Dirichlet inverse of Euler's and Liouville's functions, respectively. Show that for $n \in \mathbb{N}$, we have

(i) $\varphi^{-1}(n) = \sum_{d|n} d\mu(d) = \prod_{p|n}(1-p)$,

(ii) $\lambda^{-1}(n) = |\mu(n)|$.

2.6.24 Let $d_k(n)$ be the number of $k$-tuples $(n_1, n_2, \ldots, n_k)$ where $n_1, n_2, \ldots, n_k$ are positive integers and

$$n_1 n_2 \cdots n_k = n.$$

Show that

(i) $d_2(n) = d(n)$ is the number of positive divisors of $n$,

(ii) $d_k$ is multiplicative,

(iii) if $n = \prod_{i=1}^{\infty} p_i^{a_i}$ is the canonical factorization of $n$, then

$$d_k(n) = \prod_{i=1}^{\infty} \binom{a_i + k - 1}{k-1}.$$

2.6.25 For $k \in \mathbb{Z}$ and $n \in \mathbb{N}$, let $\sigma_k(n) = \sum_{d|n} d^k$. Show that $\sigma_k$ is multiplicative and if $n = \prod_{i=1}^{\infty} p_i^{a_i}$ is the canonical factorization of $n$, then

$$\sigma_k(n) = \prod_{i=1}^{\infty} \frac{p^{k(a_i+1)} - 1}{p^k - 1}.$$

## 2.7. Notes

To keep this chapter not too lengthy, we inevitably have to omit some important arithmetic functions, but the interested reader can find them in the books by McCarthy [**268**], Sivaramakrishnan [**373**], and Cira and Smarandache [**85**]. Here, let us mention one more additive function and two more functions which are not multiplicative but are close to being multiplicative, namely, the Alladi-Erdös function denoted by $A$, Carmichael's $\lambda$ function, and the order (or the rank) of appearance in the Fibonacci sequence, which is denoted by $z$. Notice that the same symbol is used for both Liouville's and Carmichael's functions but in this section, it always denotes the latter.

For each $n \in \mathbb{N}$, $\lambda(n)$ is the smallest positive integer $m$ such that $a^m \equiv 1 \pmod{n}$ for all $a$ that are relatively prime to $n$. Therefore, in the language of group theory, $\lambda(n)$ is the *exponent* of $(\mathbb{Z}/n\mathbb{Z})^\times$, the group of reduced residues modulo $n$. Since

$$\lambda(\operatorname{lcm}[m,n]) = \operatorname{lcm}[\lambda(m), \lambda(n)],$$

the formula for $\lambda(n)$ in terms of its values at prime powers is given by

$$\lambda(n) = \operatorname{lcm}[\lambda(p_1^{a_1}), \lambda(p_2^{a_2}), \ldots, \lambda(p_k^{a_k})], \tag{2.14}$$

where $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the canonical factorization of $n$. Its values at prime powers are also known: $\lambda(p^a) = p^a - p^{a-1} = \varphi(p^a)$ if $p$ is an odd prime and $a \geq 1$, $\lambda(2) = 1 = \varphi(2)$, $\lambda(4) = 2 = \varphi(4)$, and $\lambda(2^a) = 2^{a-2} = \varphi(2^a)/2$ for $a \geq 3$. The sequence $(\lambda(n))_{n\geq 1}$ is listed as A002322 in OEIS [**374**]. For research related to this function, Carmichael numbers, and pseudoprimes, see, for example, in the articles by Carmichael [**75**, **76**], Erdös [**116**], Pomerance [**308**], and in the book by Ribenboim [**342**, pp. 103–135].

Recall that the *Fibonacci sequence* $(F_n)_{n\geq 0}$ is defined by $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. For each positive integer $m$, $z(m)$ is smallest positive integer $k$ such that $m \mid F_k$. There are various names for the function $z$, namely, the *rank of appearance*, the *order of appearance*, the *rank of apparition*, *Fibonacci entry point*, *restricted period*, and *quasi period*. The function $z$ gained a lot of attention when Z. H. Sun and Z. W. Sun [**391**] showed that the first case of Fermat's last theorem would follow from the nonexistence of prime numbers $p$ satisfying $z(p) = z(p^2)$. From this result and a similarity between this and the Wieferich prime, the prime $p$ satisfying $z(p) = z(p^2)$ is called a *Fibonacci-Wieferich prime* or *Wall-Sun-Sun prime*. We note that Wall-Sun-Sun primes are named after D. D. Wall, Z. H. Sun and Z. W. Sun for their work in [**432**] and [**391**], respectively. Although, Fermat's last theorem was already proved by Wiles [**404**, **435**], it is still an unsolved problem whether or not there exists a Fibonacci-Wieferich prime. By running a computation in a computer, Wall [**432**], Mcintosh and Roettger [**269**], and Dorais and Klyve [**105**] observed that there is no Fibonacci-Wieferich prime $p$ in the range

$p < 10^4$, $p < 2 \times 10^{14}$, and $p < 9.7 \times 10^{14}$, respectively. For the most update information on the range of such primes $p$, see PrimeGrid Project [**330**]. For a survey on this and other related problems, we refer the reader to Klaška [**227**] and references therein.

Although numerical evidence seems to support the nonexistence of the primes $p$ with $z(p) = z(p^2)$, some mathematicians believe that such a $p$ exists. In the opposite direction, showing that there are infinitely many $p$ satisfying $z(p) \neq z(p^2)$ is nontrivial. In fact, Peng [**293**] has only recently showed that there are infinitely many non-Fibonacci-Wieferich primes by assuming a version of the famous abc-conjecture. Since this conjecture is still unsolved, Peng's theorem is conditionally true. For the reader's convenience, we state the version of the conjecture used in Peng's proof as follows.

**Conjecture 2.37.** (abc-Conjecture) For every $\varepsilon > 0$, there is a constant $C_\varepsilon > 0$ such that the inequality

$$\max\{|a|, |b|, |c|\} \leq C_\varepsilon \operatorname{rad}(abc)^{1+\varepsilon}$$

holds for all relatively prime nonzero integers $a, b, c$ with $a + b + c = 0$, where $\operatorname{rad}(abc) = \prod_{p|abc} p$.

We remark that Peng's proof was actually based on Silverman's breakthrough in [**371**], where he showed that if the abc-conjecture holds, then there are infinitely many non-Wieferich primes. Recall that a prime $p$ is called a Wieferich prime if

$$2^{p-1} \equiv 1 \pmod{p^2},$$

otherwise it is a non-Wieferich prime. It is not difficult to show that if $p$ is a Wieferich prime, then

$$2^{p^k} \equiv 2 \pmod{p^2} \quad \text{for all } k \geq 1, \tag{2.15}$$

and if (2.15) holds for some $k$, then $p$ is a Wieferich prime. Therefore, a prime $p$ is a Wieferich prime if and only if $\operatorname{ord}_{p^2} 2 = \operatorname{ord}_p 2$, which should be compared with $z(p) = z(p^2)$ in the definition of Fibonacci-Wieferich primes. So although the prime $p$ with $z(p) = z(p^2)$ has not been found, there are at least two primes $p$ satisfying $\operatorname{ord}_{p^2} 2 = \operatorname{ord}_p 2$, namely $p = 1093$ and $p = 3511$. Nevertheless, as of November 2022, the integers 1093 and 3511 are the only known Wieferich primes. There are other generalizations of Wieferich primes too. If a prime $p$ satisfies

$$a^{p-1} \equiv 1 \pmod{p^2}$$

for some integer $a \geq 2$, then $p$ is called a Wieferich prime for base $a$. In fact, Silverman [**371**] showed that if the abc-conjecture holds, then for any integer $a \geq 2$, the number of non-Wieferich primes for base $a$ that are less than or equal to $x$ is at least $c \log x$ for some absolute constant $c$ depending at most on $a$ but not on $x$. Finally, we remark that Graves and Ram Murty [**156**] extended Silverman's result by showing that for fixed integers $a, k \geq 2$, there are at least $c \log x / \log\log x$ primes $p \leq x$ such that

$$a^{p-1} \not\equiv 1 \pmod{p^2} \quad \text{and} \quad p \equiv 1 \pmod{k},$$

under the assumption of the abc-conjecture, where $c$ is an absolute constant depending at most on $a$ and $k$ but not on $x$.

Since $z(\operatorname{lcm}[m, n]) = \operatorname{lcm}[z(m), z(n)]$ the formula (2.14) also holds when $\lambda$ is replaced by $z$. That is if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the canonical factorization of $n$, then

$$z(n) = \operatorname{lcm}[z(p_1^{a_1}), z(p_2^{a_2}), \ldots, z(p_k^{a_k})].$$

If $p$ is explicitly given and not too large, then it is not difficult to evaluate $z(p^a)$ for all $a \geq 1$. However, there is no general formula for $z(p^a)$ for all $p$ and $a$, and it is therefore natural to study the behavior of the function $z$ or find the formula for $z(n)$ when $n$ is a member of a particular integer sequence. Many researchers including the author of this book have done research in this direction. For example, Marques [**260**, **261**] calculated the formula for $z(F_n \pm 1)$ and $z(F_n^k)$ for all $n \geq 3$ and $k \geq 1$. Marques [**260**] also obtained some special cases of $z(L_n^k)$ where $L_n$ is the $n$th Lucas number. Pongsriiam [**316**] then gave a complete formula for $z(L_n^k)$ for all $n, k \geq 1$. Some parts of their results are shown below.

**Theorem 2.38.** (Marques [**260**, Theorem 1.1]) *Let $n \geq 3$. Then the following statements hold.*

(i) *If $n \equiv 3 \pmod 6$, then $z(F_n^2) = nF_n$ and $z(F_n^{k+1}) = nF_n^k/2$ for $k \geq 2$.*

(ii) *If $n \not\equiv 3 \pmod 6$ and $k \geq 0$, then $z(F_n^{k+1}) = nF_n^k$.*

**Theorem 2.39.** (Pongsriiam [**316**, Theorem 1.2]) *Let $n \geq 2$. Then the following statements hold.*

(i) *$z(L_n) = 2n$.*

(ii) *If $k \geq 2$ and $n \equiv 1, 2 \pmod 3$, then $z(L_n^k) = 2nL_n^{k-1}$.*

(iii) *If $k \geq 2$ and $n \equiv 3 \pmod 6$, then $z(L_n^k) = nL_n^{k-1}$.*

(iv) *If* $k \geq 2$ *and* $n \equiv 0 \pmod 6$*, then*

$$z(L_n^k) = \begin{cases} \dfrac{nL_n^{k-1}}{2^{v_2(n)+1}}, & \text{if } k \geq v_2(n)+3; \\ \dfrac{nL_n^{k-1}}{2^{k-2}}, & \text{if } k < v_2(n)+3. \end{cases}$$

Marques [**262**, **263**] and Marques and Trojovský [**264**] computed the formulas for

$$\begin{aligned} &z(F_nF_{n+1}\cdots F_{n+k}) \quad \text{for } k = 1,2,3 \text{ and} \\ &z(L_nL_{n+1}\cdots L_{n+k}) \quad \text{for } k = 1,2,3,4 \end{aligned}$$

which were later extended by Khaochim and Pongsriiam [**220**, **221**] to the case $1 \leq k \leq 6$ with an algorithm for calculating

$$z(F_nF_{n+1}\cdots F_{n+k}) \text{ and } z(L_nL_{n+1}\cdots L_{n+k})$$

for all $k \geq 1$. While the formula for $z(F_n \pm 1)$ is known, that of $z(L_n \pm 1)$ is not. But it should be possible to calculate $z(L_n \pm 1)$ by factoring $L_n \pm 1$ as given in Pongsriiam [**317**, Lemma 2.5] and then modifying the method of Khaochim and Pongsriiam [**220**, **221**] to obtain such a formula. Pongsriiam [**320**] also gave the formula for $z(n!)$ for all $n \geq 1$ and used it to solve certain Diophantine equations involving $z(n!)$. Some parts of the results are given below. For other related results concerning the function $z$, see for example in the articles by Dorais and Klyve [**105**], Klaška [**227**], Somer and Křižek [**377**], Stewart [**384**], Z. H. Sun and Z. W. Sun [**391**], Wall [**432**], and in the online databases PrimeGrid [**330**] and OEIS [**374**].

**Theorem 2.40.** (Khaochim and Pongsriiam [**220**, Theorem 3.5]) *Let* $n \geq 1$, $a = [n, n+1, \ldots, n+5]$, $b = F_nF_{n+1}\cdots F_{n+5}$, *and* $c = (5, n)$. *Then*

$$z(b) = \begin{cases} ac, & \text{if } n \equiv 1,2,3,4,5,6 \pmod{12}, \\ & \text{or } n \equiv 7,8,59,60 \pmod{72}; \\ 2ac, & \text{if } n \equiv 9,10 \pmod{12}, \text{ or } n \equiv 23,24,43,44 \pmod{72}; \\ 3ac, & \text{if } n \equiv 11,12,31,32,35,36,55,56 \pmod{72}; \\ 6ac, & \text{if } n \equiv 0,19,20,47,48,67,68,71 \pmod{72}. \end{cases}$$

**Theorem 2.41.** (Pongsriiam [**320**, Corollary 3.14]) *Suppose that* $v_p(F_{z(p)}) = 1$ *for all p. Then for all* $m \geq 8$,

$$z(m!\,) = \frac{5m!\left(\frac{m+1}{2}\right)^{\delta}}{2\prod\limits_{p\leq m} p}, \quad \textit{where}$$

$$\delta = \begin{cases} 1, & \textit{if } m \textit{ and } \frac{m+1}{2} \textit{ are primes and } \frac{m+1}{2} \equiv 2, 4 \pmod 5; \\ 0, & \textit{otherwise.} \end{cases}$$

The assumption $v_p(F_{z(p)}) = 1$ for all $p$ in Theorem 2.41 is a very strong condition. In fact, it is an open problem which is equivalent to the nonexistence of prime $p$ satisfying the aforementioned Diophantine equation $z(p) = z(p^2)$. Nevertheless, Pongsriiam [**320**] also gave the formula for $z(n!\,)$ without assuming $v_p(F_{z(p)}) = 1$ for all $p$ but it is more complicated.

Some local behaviors of $z(m)$ were obtained by Luca and Pomerance in [**252**] where they showed that the Diophantine equation

$$z(n) = z(n+1)$$

has infinitely many solutions and the inequality

$$z(m) < z(m+1) < z(m+2)$$

and any other permutation of $z(m), z(m+1), z(m+2)$ hold for infinitely many $m$. It is well known that $z(p) \leq p+1$ for all primes $p$ but it is not known if there are infinitely many $p$ such that $z(p) = p+1$. Are there infinitely many $m$ such that

$$z(m) < z(m+1) < z(m+2) < z(m+3)?$$

Does the above inequality hold for infinitely many $m$ if we replace $z(m)$, $z(m+1)$, $z(m+2)$, $z(m+3)$ by its permutation? Are there infinitely many $m$ such that

$$z(m) = z(m+1) = z(m+2)?$$

Can we find a closed formula for $z(F_m \pm 2)$ for all $m$? Luca and Pomerance proposed the following conjecture:

**Conjecture 2.42.** (Luca and Pomerance [**252**]) For all integers $k \geq 2$ and all permutations $\sigma \in S_k$, there exist infinitely many $m$ such that

$$z(m+\sigma(1)) < z(m+\sigma(2)) < \cdots < z(m+\sigma(k)).$$

Lagarias [**236**, **237**] proved in 1985 that the density of primes $p$ satisfying $z(p) \equiv 0 \pmod 2$ is 2/3. More precisely, if $\pi(x)$ is the number of primes less than or equal to $x$ and $A(x, m, a)$ is the number of primes $p \leq x$ such that $z(p) \equiv a \pmod m$, then

$$\lim_{x\to\infty} \frac{A(x,2,0)}{\pi(x)} = \frac{2}{3}.$$

Bruckman and Anderson [**63**] gathered numerical data and made a conjecture on a formula for $\lim_{x\to\infty} \frac{A(x,m,0)}{\pi(x)}$ when $m \geq 3$. About 15 years after Bruckman and Anderson, and 28 years after Lagarias, Cubre and Rouse [**95**] completely solved this problem. Their results are as follows.

**Theorem 2.43.** (Cubre and Rouse [**95**]) *For each $m \geq 2$, let*

$$D(m) = \lim_{x\to\infty} \frac{A(x,m,0)}{\pi(x)},$$

*$\rho(m) = 1$ if $10 \nmid m$, $\rho(m) = 5/4$ if $m \equiv 10 \pmod{20}$, and $\rho(m) = 1/2$ if $20 \mid m$. Then for each prime $q$ and positive integer $e$, we have $D(q^e) = \frac{q^{2-e}}{q^2-1}$. Moreover, for each positive integer $m$,*

$$D(m) = \rho(m) \prod_{q^j \| m} D(q^j).$$

**Theorem 2.44.** (Cubre and Rouse [**95**]) *Let $p$ be a prime and let $\varepsilon_p = \left(\frac{p}{5}\right)$ be the Legendre symbol. Given a prime $q$ and integers $x$, $i$, and $j$ with $i \geq j \geq 0$, let $M(q, x, i, j)$ denote the number of primes $p \leq x$ such that $q^i \parallel (p - \varepsilon_p)$ and $q^j \parallel z(p)$. Then*

$$\lim_{x\to\infty} \frac{M(q,x,i,j)}{\pi(x)} = \begin{cases} \frac{q-2}{q-1}, & \textit{if } i = j = 0; \\ q^{-2i}, & \textit{if } i \geq 1 \textit{ and } j = 0; \\ \frac{q-1}{q^{2i-j+1}}, & \textit{otherwise.} \end{cases}$$

Perhaps, the next step is to consider the limit, when $0 < a < m$,

$$D(m,a) = \lim_{x\to\infty} \frac{A(x,m,a)}{\pi(x)}.$$

There are various generalizations of the Fibonacci numbers. One way is to consider the Lucas sequences of the first and second kinds which depend on parameters $a, b \in \mathbb{Z}$ and are defined, respectively, by the recurrences

$$u_0 = 0, u_1 = 1, \text{ and } u_n = au_{n-1} + bu_{n-2} \quad \text{for } n \geq 2,$$
$$v_0 = 2, v_1 = a, \text{ and } v_n = av_{n-1} + bv_{n-2} \quad \text{for } n \geq 2.$$

So if $a = b = 1$, then $(u_n)$ and $(v_n)$ reduce to the classical sequences of Fibonacci and Lucas numbers; if $a = 6$ and $b = -1$, then they become the sequences of balancing and Lucas-balancing numbers; if $a = 2$ and $b = 1$, then they are the sequences of Pell and Pell-Lucas numbers; and many other famous integer sequences are just a special case of $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$. The order of appearance of $n$ in the Lucas sequence of the first kind, denoted by $\tau(n)$, is defined to be the smallest positive integer $k$ such that $n \mid u_k$. Perhaps, all results concerning $z$ and $(F_n)_{n\geq 0}$ can be generalized to the case of $\tau$ and $(u_n)_{n\geq 0}$. To summarize, the following questions are open and interesting:

(i) Is it possible to find a closed form for $D(m, a)$ when $0 < a < m$?

(ii) Is Conjecture 2.42 true? Can we at least prove it for small values of $k$?

(iii) Can we find formulas for $z(F_n \pm k)$ and $z(L_n \pm k)$ for all large $n$?

(iv) Can we explicitly give a prime $p$ with $z(p) = z(p^2)$?

(v) What are the corresponding results when we replace $z$ and $(F_n)_{n\geq 0}$ by $\tau$ and $(u_n)_{n\geq 0}$ in Theorems 2.38 to 2.41?

Finally, for each $n \in \mathbb{N}$, the *Alladi-Erdös function* is defined by

$$A(n) = \sum_{p^a \| n} ap,$$

that is, $A(n)$ is the sum of all prime divisors of $n$ counted with multiplicity. This was first studied in detail by Alladi and Erdös [**4**]; see also the references therein for some of the work before [**4**]. One of the entertaining facts associated with this function is that Aaron hit the 715th home run beating Ruth's record of 714 and Pomerance noted that $714 = 2 \times 3 \times 7 \times 17$ and $715 = 5 \times 11 \times 13$ contained the first seven primes and that $A(714) = A(715)$. Pomerance [**309**] called the positive integer $n$ such that $A(n) = A(n+1)$ a *Ruth-Aaron number* and showed that the number of $n \leq x$ with $A(n) = A(n+1)$ is $O(x(\log\log x)^4/(\log x)^2)$. However, whether or not there are infinitely many Ruth-Aaron numbers is still open. The sequence of Ruth-Aaron numbers is given as A039752 in OEIS. If the multiplicity is not counted, that is, if $A'(n) = \sum_{p|n} p$, then the sequence of $n$ such that $A'(n) = A'(n+1)$ is listed as A006145 in OEIS.

## Chapter 3

# The Floor Function

## 3.1. Introduction

The origin of the greatest integer function is difficult to establish but it has been found quite commonly in the literature since the 1880s. Gauss, Dirichlet, Legendre, Sylvester, Kronecker, and many other mathematicians used it. A brief history of this function and a collection of its basic properties can also be found in the master theses by Murray [**279**] and by Haertel [**166**]. There were two popular symbols for the largest integer not exceeding $x$, namely $E(x)$ and $[x]$. Then Iverson [**210**] introduced in 1962 a new name and notation for this function which are now more popular and widely used in number theory and combinatorics. In this text, we follow Iverson and use $\lfloor x \rfloor$ instead of $E(x)$ or $[x]$, and call it the floor function. The definition of the floor and related functions are given as follows:

**Definition 3.1.** For each $x \in \mathbb{R}$, let $\lfloor x \rfloor$ be the largest integer less than or equal to $x$ and let $\lceil x \rceil$ be the smallest integer larger than or equal to $x$. We call $\lfloor x \rfloor$ the *floor function* (or the *greatest integer function*) of $x$ and call $\lceil x \rceil$ the *ceiling function* (or the *least integer function*) of $x$. In addition, we define $\{x\} = x - \lfloor x \rfloor$ and call $\{x\}$ the *fractional part* of $x$. Moreover, $\lfloor x \rfloor$ is sometimes called the *integer part* of $x$.

For instance, we have $\lfloor 2.5 \rfloor = 2$, $\lceil 2.5 \rceil = 3$, $\{2.5\} = 0.5$, $\lfloor -3.1 \rfloor = -4$, $\lceil -3.1 \rceil = -3$, $\{-3.1\} = 0.9$, $\lfloor \pi \rfloor = 3$, $\lceil \pi \rceil = 4$, and $\{\pi\} = \pi - 3$. Iverson also introduced another notation using a bracket which is not used often in this book but is a very convenient tool in some calculations. See the notes in Section 3.6 for more details.

**Definition 3.2.** If $P$ is a mathematical statement, then the *Iverson bracket* $[P]$ is defined by

$$[P] = \begin{cases} 1, & \text{if } P \text{ is true;} \\ 0, & \text{if } P \text{ is false.} \end{cases}$$

So, for example, [2 is a prime] $= 1$, [5 is composite] $= 0$, and $[2+5 = 7] = 1$.

The following are basic properties of the floor and ceiling functions, which are applied throughout this chapter, sometimes without reference.

**Theorem 3.3.** *Let $x$, $y$ be real numbers and let $m$, $n$ be integers. Then the following statements hold.*

(i) $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$, $\lceil x \rceil - 1 < x \le \lceil x \rceil$, *and* $0 \le \{x\} < 1$. *In fact,* $\lfloor x \rfloor$ *is the unique integer* $n$ *such that* $n \le x < n + 1$. *Similarly,* $\lceil x \rceil$ *is the unique integer satisfying*

$$\lceil x \rceil - 1 < x \le \lceil x \rceil .$$

(ii) $\lfloor x \rfloor = x \Leftrightarrow x \in \mathbb{Z} \Leftrightarrow \lceil x \rceil = x$,

$$\lfloor x \rfloor = n \Leftrightarrow n \le x < n+1 \Leftrightarrow x - 1 < n \le x,$$
$$\lceil x \rceil = n \Leftrightarrow n - 1 < x \le n \Leftrightarrow x \le n < x + 1.$$

(iii) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, $\lceil x + n \rceil = \lceil x \rceil + n$, $\{x + n\} = \{x\}$.

(iv) $\lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ 1, & \text{if } x \notin \mathbb{Z}. \end{cases}$

(v) $\lfloor -x \rfloor = -\lceil x \rceil$, $\lceil -x \rceil = -\lfloor x \rfloor$,

$$\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor, & \text{if } x \in \mathbb{Z}; \\ -\lfloor x \rfloor - 1, & \text{if } x \notin \mathbb{Z}, \end{cases}$$

$$\lceil -x \rceil = \begin{cases} -\lceil x \rceil, & \text{if } x \in \mathbb{Z}; \\ -\lceil x \rceil + 1, & \text{if } x \notin \mathbb{Z}. \end{cases}$$

$$\{-x\} = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ 1 - \{x\}, & \text{if } x \notin \mathbb{Z}. \end{cases}$$

$\left\lfloor x + \frac{1}{2} \right\rfloor$ *is the nearest integer to* $x$. *If two integers are equally near to* $x$, *it is the larger of the two. In addition,* $-\left\lfloor -x + \frac{1}{2} \right\rfloor$ *is* *the nearest integer to* $x$ *and if two integers are equally near to* $x$*, it is the smaller of the two.*

(vi) *The floor and ceiling functions are increasing on* $\mathbb{R}$ (*but are not strictly increasing on* $\mathbb{R}$). *That is,*

$$x < y \text{ implies } \lfloor x \rfloor \le \lfloor y \rfloor \text{ and } \lceil x \rceil \le \lceil y \rceil .$$

*In addition, we have*

$$\begin{aligned} x < n &\Leftrightarrow \lfloor x \rfloor < n, \\ x \ge n &\Leftrightarrow \lfloor x \rfloor \ge n, \\ x \le n &\Leftrightarrow \lceil x \rceil \le n, \\ x > n &\Leftrightarrow \lceil x \rceil > n. \end{aligned}$$

(vii) $0 \le \lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \le 1$. *More precisely,*

$$\lfloor x+y \rfloor = \begin{cases} \lfloor x \rfloor + \lfloor y \rfloor, & \text{if } \{x\}+\{y\} < 1; \\ \lfloor x \rfloor + \lfloor y \rfloor + 1, & \text{if } \{x\}+\{y\} \ge 1. \end{cases}$$

(viii) $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$ *and* $\left\lceil \frac{\lceil x \rceil}{n} \right\rceil = \left\lceil \frac{x}{n} \right\rceil$ *for* $n \ge 1$.

**Proof.** We begin with (i). By the definition of $\lfloor x \rfloor$, we immediately obtain the inequality $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$ and by this and the definition of $\{x\}$, we see that $0 \le \{x\} < 1$. Similarly, $\lceil x \rceil - 1 < x \le \lceil x \rceil$. If $n$ is an integer satisfying, $n \le x < n+1$, then $n$ is the largest integer that is less than or equal to $x$, and so $n = \lfloor x \rfloor$. The uniqueness of $\lceil x \rceil$ can be obtained similarly. This proves (i). Then (ii) follows immediately from (i). Since (iii) to (vi) can be proved by using a similar idea, we only give a proof of (iv) and some parts of (v).

For (iv), if $x \in \mathbb{Z}$, then the result is easily verified. So suppose $x \notin \mathbb{Z}$. Then $m < x < m+1$ for some $m \in \mathbb{Z}$. Then

$$\lceil x \rceil - \lfloor x \rfloor = (m+1) - m = 1,$$

which proves (iv). In addition, $-m-1 < -x < -m$, so

$$\lfloor -x \rfloor = -m-1 = -\lfloor x \rfloor - 1, \quad \lceil -x \rceil = -m = -\lceil x \rceil + 1,$$

which proves some parts of (v). The rest of (iii) to (vi) is left to the reader.

For (vii), suppose that $m \le x < m+1$ and $n \le y < n+1$. Then $m+n \le x+y < m+n+2$. Therefore $\lfloor x+y \rfloor = m+n$ or $m+n+1$, which are $\lfloor x \rfloor + \lfloor y \rfloor$ or $\lfloor x \rfloor + \lfloor y \rfloor + 1$, respectively. This proves the first part of (vii). More precisely, we have

$$\begin{aligned}\lfloor x+y \rfloor &= \begin{cases} m+n, & \text{if } m+n \le x+y < m+n+1; \\ m+n+1, & \text{if } m+n+1 \le x+y \end{cases} \\ &= \begin{cases} \lfloor x \rfloor + \lfloor y \rfloor, & \text{if } \lfloor x \rfloor + \lfloor y \rfloor \le x+y < \lfloor x \rfloor + \lfloor y \rfloor + 1; \\ \lfloor x \rfloor + \lfloor y \rfloor + 1, & \text{if } \lfloor x \rfloor + \lfloor y \rfloor + 1 \le x+y \end{cases} \\ &= \begin{cases} \lfloor x \rfloor + \lfloor y \rfloor, & \text{if } 0 \le x - \lfloor x \rfloor + y - \lfloor y \rfloor < 1; \\ \lfloor x \rfloor + \lfloor y \rfloor + 1, & \text{if } 1 \le x - \lfloor x \rfloor + y - \lfloor y \rfloor \end{cases} \\ &= \begin{cases} \lfloor x \rfloor + \lfloor y \rfloor, & \text{if } 0 \le \{x\} + \{y\} < 1; \\ \lfloor x \rfloor + \lfloor y \rfloor + 1, & \text{if } \{x\} + \{y\} \ge 1. \end{cases}\end{aligned}$$

Next, we prove (viii). Assume that $m \in \mathbb{Z}$ and $m \le x < m+1$. By the division algorithm, we can write $m = nq + r$ where $q, r \in \mathbb{Z}$ and $0 \le r < n$. Then

$$q \le q + \frac{r}{n} = \frac{m}{n} \le \frac{x}{n} < \frac{m}{n} + \frac{1}{n} = q + \frac{r}{n} + \frac{1}{n} \le q + \frac{n-1}{n} + \frac{1}{n} = q + 1.$$

Therefore $\left\lfloor \frac{x}{n} \right\rfloor = q$. We also have $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{m}{n} \right\rfloor = \left\lfloor q + \frac{r}{n} \right\rfloor = q$. Hence $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$. Similarly, $\left\lceil \frac{x}{n} \right\rceil = \left\lceil \frac{\lceil x \rceil}{n} \right\rceil$. This completes the proof. ☐

Some of the above properties can be extended. For example, Theorem 3.3(vii) can be generalized to three or more variables:

$$0 \le \left\lfloor \sum_{i=1}^{n} x_i \right\rfloor - \sum_{i=1}^{n} \lfloor x_i \rfloor \le n-1.$$

See also those given in the exercise. In addition, an extension in the form of the inclusion-exclusion principle is given in the article by Onphaeng and Pongsriiam [**291**]; see more details in the notes at the end of this chapter. Furthermore, McEliece made an observation which led to a generalization of Theorem 3.3(viii) and it was recorded in the book by Graham, Knuth, and Patashnik [**152**]. The result is as follows.

**Theorem 3.4.** [**152**, p. 71] *Let $I$ be an interval and let $f : I \to \mathbb{R}$ be continuous and increasing on $I$. Suppose that for each $x \in I$, $f(x) \in \mathbb{Z}$ implies $x \in \mathbb{Z}$. Then $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$ and $\lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil$ whenever $f(x)$, $f(\lfloor x \rfloor)$, and $f(\lceil x \rceil)$ are defined.*

**Proof.** We only show that $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$ since the other case is similar and is already proved in [**152**, p. 71]. If $x \in \mathbb{Z}$, then $x = \lfloor x \rfloor$ and we are done. So assume that $x \notin \mathbb{Z}$. Since $\lfloor x \rfloor < x$ and $f$ is increasing, we have $f(\lfloor x \rfloor) \leq f(x)$. So $\lfloor f(\lfloor x \rfloor) \rfloor \leq \lfloor f(x) \rfloor$. Suppose for a contradiction that $\lfloor f(\lfloor x \rfloor) \rfloor < \lfloor f(x) \rfloor$. Since $f(\lfloor x \rfloor) \leq f(x)$ but $\lfloor f(\lfloor x \rfloor) \rfloor < \lfloor f(x) \rfloor$, we see that there is an integer $m$ satisfying

$$f(\lfloor x \rfloor) < m \leq f(x).$$

Since $f$ is continuous, we obtain by the intermediate value theorem that there is $y \in I$ such that $\lfloor x \rfloor < y \leq x$ and $f(y) = m$. By the assumption on $f$, we see that $y \in \mathbb{Z}$, which contradicts the fact that there is no integer in the interval $(\lfloor x \rfloor, x]$. So the proof is complete. ☐

**Corollary 3.5.** *For each $x \in \mathbb{R}$, $m \in \mathbb{Z}$, and $n \in \mathbb{N}$, we have*

$$\left\lfloor \frac{x+m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + m}{n} \right\rfloor \quad \textit{and} \quad \left\lceil \frac{x+m}{n} \right\rceil = \left\lceil \frac{\lceil x \rceil + m}{n} \right\rceil.$$

**Proof.** This follows immediately by applying Theorem 3.4 to the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \frac{x+m}{n}$. ☐

Next, we show the calculations involving the floor and ceiling functions in various examples.

**Example 3.6.** Let $a, b \in \mathbb{N}$. By the division algorithm, there are $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$. Show that $q = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - b\left\lfloor \frac{a}{b} \right\rfloor$. We remark that we also write $a \bmod b$ to denote $r$.

**Solution.** We have $a/b = q + r/b$ and $0 \leq r/b < 1$. Therefore $\lfloor a/b \rfloor = q$ by Theorem 3.3(iii). Then $r = a - bq = a - b\lfloor a/b \rfloor$. ☐

**Example 3.7.** Show that for all $x \geq 0$, we have

$$\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \left\lfloor \sqrt{x} \right\rfloor \quad \text{and} \quad \left\lceil \sqrt{\lceil x \rceil} \right\rceil = \left\lceil \sqrt{x} \right\rceil.$$

Show also that for $x \geq 0$,

(i) $\left\lceil \sqrt{x} \right\rceil = \left\lfloor \sqrt{\lceil x \rceil} \right\rfloor$ if and only if $x \in \{0\} \cup \bigcup_{m=1}^{\infty} (m^2 - 1, m^2]$,

(ii) $\left\lfloor \sqrt{x} \right\rfloor = \left\lceil \sqrt{\lfloor x \rfloor} \right\rceil$ if and only if $x \in \bigcup_{m=0}^{\infty} [m^2, m^2 + 1)$.

**Solution.** By applying Theorem 3.4 to the function

$$f : [0, \infty) \to [0, \infty) \text{ given by } f(x) = \sqrt{x},$$

we immediately obtain the first part. Nevertheless, let us give a direct proof of the equality $\left\lfloor\sqrt{\lfloor x\rfloor}\right\rfloor = \left\lfloor\sqrt{x}\right\rfloor$ since it gives an idea of how to prove (i) and (ii).

Suppose that $\left\lfloor\sqrt{x}\right\rfloor = n$ for some $n \in \mathbb{N}\cup\{0\}$. Then we apply usual algebraic manipulations together with (ii) and (vi) of Theorem 3.3 to obtain the following inequalities:

$$\begin{gathered} n \le \sqrt{x} < n+1, \quad n^2 \le x < (n+1)^2, \\ n^2 \le \lfloor x\rfloor < (n+1)^2, \quad \text{and} \quad n \le \sqrt{\lfloor x\rfloor} < n+1. \end{gathered}$$

The last inequality implies that $\left\lfloor\sqrt{\lfloor x\rfloor}\right\rfloor = n$. Therefore

$$\left\lfloor\sqrt{\lfloor x\rfloor}\right\rfloor = \left\lfloor\sqrt{x}\right\rfloor \text{ for all } x \ge 0,$$

as desired. Alternatively, we begin by letting $\left\lfloor\sqrt{\lfloor x\rfloor}\right\rfloor = n$, which leads us to the following inequalities:

$$\begin{gathered} n \le \sqrt{\lfloor x\rfloor} < n+1,\ n^2 \le \lfloor x\rfloor < (n+1)^2, \\ n^2 \le x < (n+1)^2,\ n \le \sqrt{x} < n+1, \end{gathered}$$

and the last inequality implies that $\left\lfloor\sqrt{x}\right\rfloor = n = \left\lfloor\sqrt{\lfloor x\rfloor}\right\rfloor$. Next we prove (i). So assume that $\left\lceil\sqrt{x}\,\right\rceil = \left\lfloor\sqrt{\lceil x\rceil}\right\rfloor$ and $x \neq 0$. Then $(m-1)^2 < x \le m^2$ for some $m \ge 1$. By a similar calculation, we obtain

$$\left\lceil\sqrt{x}\,\right\rceil = m \quad \text{and} \quad m-1 < \sqrt{\lceil x\rceil} \le m.$$

Since $\left\lfloor\sqrt{\lceil x\rceil}\right\rfloor = \left\lceil\sqrt{x}\,\right\rceil = m$, we see that $\sqrt{\lceil x\rceil} = m$, which implies $m^2 - 1 < x \le m^2$ as required. Noting that $(m-1)^2 \le m^2 - 1$, we obtain the converse of (i) by a direct calculation. The proof of (ii) is similar. □

**Example 3.8.** Show that for each $m \in \mathbb{Z}$,

$$\left\lfloor \frac{m - \left\lfloor \frac{m-17}{25} \right\rfloor}{3} \right\rfloor = \left\lfloor \frac{8m+13}{25} \right\rfloor. \tag{3.1}$$

**Solution.** Let $m \in \mathbb{Z}$. Since the set $A =: \{17, 18, \ldots, 41\}$ is a complete residue system modulo 25, there are $q \in \mathbb{Z}$ and $r \in A$ such that $m = 25q + r$. Then $\left\lfloor \frac{m-17}{25} \right\rfloor = \left\lfloor q + \frac{r-17}{25} \right\rfloor = q$ and the left-hand side of (3.1) is $\left\lfloor \frac{m-q}{3} \right\rfloor = 8q + \left\lfloor \frac{r}{3} \right\rfloor$. The right-hand side of (3.1) is $\left\lfloor 8q + \frac{8r+13}{25} \right\rfloor =$

$8q + \left\lfloor \frac{8r+13}{25} \right\rfloor$. So it suffices to show that $\left\lfloor \frac{r}{3} \right\rfloor = \left\lfloor \frac{8r+13}{25} \right\rfloor$ for all $r \in A$. Let $r \equiv a \pmod 3$ where $a = 0, 1, 2$. Then

$$\left\lfloor \frac{r}{3} \right\rfloor = \frac{r-a}{3} \quad \text{and}$$
$$\left\lfloor \frac{8r+13}{25} \right\rfloor = \left\lfloor \frac{r}{3} + \frac{39-r}{75} \right\rfloor = \frac{r-a}{3} + \left\lfloor \frac{39-r}{75} + \frac{a}{3} \right\rfloor.$$

So it is enough to show that $0 < \frac{39-r}{75} + \frac{a}{3} < 1$. If $r < 39$, then it is $> 0$ and if $r = 40, 41$, then we can check it directly. In addition, $\frac{39-r}{75} + \frac{a}{3} \leq \frac{39-17}{75} + \frac{2}{3} < 1$. So the proof is complete. Alternatively, we can use the result in Exercise 3.5.5 to solve this problem. The details are left to the reader. ☐

## 3.2. Hermite's Identity and Generalizations

Formulas for sums involving the floor function have been of interest for many years, going back at least to 1890 (see e.g. [**70**]). A famous problem in number theory is to estimate the sum

$$\sum_{n \leq N} d(n) = \sum_{n \leq N} \left\lfloor \frac{N}{n} \right\rfloor$$

with an error term as small as possible. Here $d(n)$ is the number of positive divisors of $n$. It is well known that the sum is approximately $N \log N + (2\gamma - 1)N$ with an error $O\left(N^{\theta}\right)$, where $\gamma$ is Euler's constant and $\frac{1}{4} \leq \theta \leq \frac{1}{2}$, and it is conjectured that we can take $\theta = \frac{1}{4} + \varepsilon$ for any $\varepsilon > 0$. We give more details about this in Chapter 5. In this section, we consider a more elementary sum. The notations

$$\sum_{a \leq k \leq b} f(k), \quad \sum_{a \leq k < b} f(k), \quad \sum_{a < k \leq b} f(k), \quad \sum_{a < k < b} f(k), \quad \sum_{k \leq x} f(k)$$

mean that the sums are taken over the integers $k$ lying in the intervals $[a, b]$, $[a, b)$, $(a, b]$, $(a, b)$, and $[1, x]$, respectively. One of the simple but beautiful formulas for sums involving the floor function is that of Hermite.

**Theorem 3.9.** (Hermite's identity) *For each $x \in \mathbb{R}$ and $n \in \mathbb{N}$,*

$$\sum_{0 \leq k \leq n-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \lfloor nx \rfloor.$$

There are many ways to prove Hermite's identity. Here we give a proof of a more general result as shown in Aursukaree et al. [**20**].

**Theorem 3.10.** (Aursukaree et al. [**20**]) *Let $x \in \mathbb{R}$, $m, n \in \mathbb{Z}$, and $0 \leq m \leq n$. Then*

$$\sum_{0 \leq k \leq m-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \max\{m \lfloor x \rfloor, m \lfloor x \rfloor + m - n + \lfloor n\{x\} \rfloor\}. \tag{3.2}$$

*In particular, if $m = n$ are positive integers, then* (3.2) *is the same as Hermite's identity.*

**Proof.** Since $n\{x\} < n$, we have $-n + \lfloor n\{x\} \rfloor < 0$. When $m = 0$, the left-hand side of (3.2) is an empty sum and so it is equal to 0, and the right-hand side of (3.2) is also equal to $\max\{0, -n + \lfloor n\{x\} \rfloor\} = 0$. Therefore assume that $m \geq 1$. Then

$$\left\lfloor x + \frac{k}{n} \right\rfloor = \left\lfloor \lfloor x \rfloor + \{x\} + \frac{k}{n} \right\rfloor = \lfloor x \rfloor + \left\lfloor \frac{n\{x\} + k}{n} \right\rfloor.$$

So the left-hand side of (3.2) is equal to

$$m \lfloor x \rfloor + \sum_{0 \leq k \leq m-1} \left\lfloor \frac{n\{x\} + k}{n} \right\rfloor.$$

Since $0 \leq n\{x\} < n$, there exists $r \in \{0, 1, 2, \ldots, n-1\}$ such that $r \leq n\{x\} < r + 1$. So $r = \lfloor n\{x\} \rfloor$. For $0 \leq k \leq m - 1$, we have

$$0 \leq \frac{k}{n} \leq \frac{n\{x\} + k}{n} < \frac{n + k}{n} < 2.$$

So $\left\lfloor \frac{n\{x\}+k}{n} \right\rfloor = 0$ or 1. In addition, $\left\lfloor \frac{n\{x\}+k}{n} \right\rfloor = 1 \Leftrightarrow \frac{n\{x\}+k}{n} \geq 1$. If $k \geq n - r$, then $\frac{n\{x\}+k}{n} \geq \frac{n+n\{x\}-r}{n} \geq 1$. If $k < n - r$, then $\frac{n\{x\}+k}{n} \leq \frac{n\{x\}+n-r-1}{n} < 1$. Therefore $\left\lfloor \frac{n\{x\}+k}{n} \right\rfloor = 1$ if and only if $k \geq n - r$. Therefore

$$\begin{aligned} \sum_{0 \leq k \leq m-1} \left\lfloor \frac{n\{x\} + k}{n} \right\rfloor &= \sum_{n-r \leq k \leq m-1} 1 \\ &= \begin{cases} m - n + r, & \text{if } m \geq n - r + 1; \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Therefore the left-hand side of (3.2) is equal to $m \lfloor x \rfloor + m - n + r$ if $m - n + r \geq 1$, and is equal to $m \lfloor x \rfloor$ if $m - n + r \leq 0$. By recalling that $r = \lfloor n\{x\} \rfloor$, the result follows. ☐

There are various ways to extend Theorem 3.10 further. For example, we can change the range of $k$ in the index of summation as shown in Theorem 3.11, Corollary 3.12, and Theorem 3.13. In Theorem 3.11, the restriction $0 \le m \le n$ in Theorem 3.10 is removed.

**Theorem 3.11.** (Aursukaree et al. [**20**]) *Let $x \in \mathbb{R}$ and $m, n \in \mathbb{N}$. Then*

$$\sum_{0 \le k \le m-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \frac{n}{2} \left\lfloor \frac{m}{n} \right\rfloor \left( \left\lfloor \frac{m}{n} \right\rfloor - 1 \right) + \left\lfloor \frac{m}{n} \right\rfloor \lfloor nx \rfloor + \left\lfloor \frac{m}{n} \right\rfloor r$$
$$+ \max\{r \lfloor x \rfloor, r \lfloor x \rfloor + r - n + \lfloor n\{x\} \rfloor\},$$

*where $r = m - n \left\lfloor \frac{m}{n} \right\rfloor$ is the remainder in the division of $m$ by $n$.*

**Proof.** Since the case $m \le n$ is already proved in Theorem 3.10, we can assume that $m > n$. By the division algorithm, there exist $q \in \mathbb{N}$ and $r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \le r < n$. Then $\left\lfloor \frac{m}{n} \right\rfloor = \left\lfloor q + \frac{r}{n} \right\rfloor = q + \left\lfloor \frac{r}{n} \right\rfloor = q$ and $r = m - nq = m - n \left\lfloor \frac{m}{n} \right\rfloor$. Then we have

$$\sum_{0 \le k \le m-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \sum_{\ell=0}^{q-1} \sum_{\ell n \le k \le (\ell+1)n-1} \left\lfloor x + \frac{k}{n} \right\rfloor$$
$$+ \sum_{qn \le k \le qn+r-1} \left\lfloor x + \frac{k}{n} \right\rfloor.$$

By replacing $k$ by $k + \ell n$ in the first sum and $k$ by $k + qn$ in the second sum on the right-hand side of the above equation, we see that

$$\sum_{0 \le k \le m-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \sum_{\ell=0}^{q-1} \sum_{0 \le k \le n-1} \left\lfloor x + \frac{k + \ell n}{n} \right\rfloor$$
$$+ \sum_{0 \le k \le r-1} \left\lfloor x + \frac{k + qn}{n} \right\rfloor. \tag{3.3}$$

Since $\left\lfloor x + \frac{k+\ell n}{n} \right\rfloor = \left\lfloor x + \frac{k}{n} + \ell \right\rfloor = \ell + \left\lfloor x + \frac{k}{n} \right\rfloor$, we obtain by Theorem 3.10 that the first sum on the right-hand side of (3.3) is

$$\sum_{\ell=0}^{q-1} \left( n\ell + \sum_{0 \le k \le n-1} \left\lfloor x + \frac{k}{n} \right\rfloor \right) = \sum_{\ell=0}^{q-1} (n\ell + \lfloor nx \rfloor) \tag{3.4}$$
$$= \frac{nq(q-1)}{2} + q \lfloor nx \rfloor.$$

The second sum can also be evaluated by Theorem 3.10 and it is equal to

$$qr + \max\{r\lfloor x\rfloor, r\lfloor x\rfloor + r - n + \lfloor n\{x\}\rfloor\}. \tag{3.5}$$

Recall that $q = \left\lfloor \frac{m}{n} \right\rfloor$ and $r = m - n\left\lfloor \frac{m}{n} \right\rfloor$ is the remainder in the division of $m$ by $n$. Then substituting (3.4) and (3.5) in (3.3) leads to the desired result. □

The index of summation can be extended to the integers $k$ from $a$ to $b$ for any $a < b$ as follows.

**Corollary 3.12.** (Aursukaree et al. [**20**]) *Let $x \in \mathbb{R}$, $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ and $a < b$. Then*

$$\sum_{a \le k < b} \left\lfloor x + \frac{k}{n} \right\rfloor = \frac{n}{2}\left\lfloor \frac{m}{n} \right\rfloor\left(\left\lfloor \frac{m}{n} \right\rfloor - 1\right) + \left\lfloor \frac{m}{n} \right\rfloor r + \left\lfloor \frac{m}{n} \right\rfloor \lfloor nx \rfloor$$
$$+ \left\lfloor \frac{m}{n} \right\rfloor a + \max\left\{r\left\lfloor x + \frac{a}{n} \right\rfloor, r\left\lfloor x + \frac{a}{n} \right\rfloor + r - n + \left\lfloor n\left\{x + \frac{a}{n}\right\}\right\rfloor\right\},$$

*where $m = b - a$ and $r$ is the remainder in the division of $b - a$ by $n$.*

**Proof.** Replacing $k$ by $k + a$, we see that the left-hand side is

$$\sum_{0 \le k < b-a} \left\lfloor \left(x + \frac{a}{n}\right) + \frac{k}{n} \right\rfloor,$$

which is suitable for an application of Theorem 3.11. This leads to the desired result. □

The third form of the extension of Hermite's identity is to change $k$ in the summand to range over the complete system of residues modulo $n$ as shown in the next theorem.

**Theorem 3.13.** (Aursukaree et al. [**20**]) *Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Assume that the set $\{a_0, a_1, \ldots, a_{n-1}\}$ is a complete residue system modulo $n$. Then*

$$\sum_{0 \le k \le n-1} \left\lfloor x + \frac{a_k}{n} \right\rfloor = \lfloor nx \rfloor - \frac{n-1}{2} + \frac{1}{n}\sum_{k=0}^{n-1} a_k.$$

*In particular, if $\{a_0, a_1, \ldots, a_{n-1}\} = \{0, 1, \ldots, n-1\}$, then this is the same as Hermite's identity.*

**Proof.** We can assume without loss of generality that for each $k = 0, 1, \ldots, n-1$, we have $a_k \equiv k \pmod{n}$. Then $(a_k - k)/n$ is an integer and we obtain that

$$\left\lfloor x + \frac{a_k}{n} \right\rfloor = \left\lfloor x + \frac{a_k - k}{n} + \frac{k}{n} \right\rfloor = \frac{a_k - k}{n} + \left\lfloor x + \frac{k}{n} \right\rfloor.$$

From this and Theorem 3.10, we see that the sum in question is equal to

$$\frac{1}{n}\left(\sum_{0\le k\le n-1} (a_k - k)\right) + \lfloor nx \rfloor = \lfloor nx \rfloor - \frac{n-1}{2} + \frac{1}{n}\sum_{k=0}^{n-1} a_k. \qquad \square$$

See also Exercise 3.5.17 for another generalization of Hermite's identity. Some applications of Hermite's identity are shown in the following examples.

**Example 3.14.** Let $n \in \mathbb{N}$ and for each $x \in \mathbb{R}$, let $f(x) = x - \lfloor x \rfloor - \frac{1}{2}$. We call $f$ saw–tooth function and sometimes denotes $f(x)$ by $((x))$. Show that

$$\sum_{k=0}^{n-1} f\left(x + \frac{k}{n}\right) = f(nx).$$

**Solution.** By Hermite's identity, the left-hand side of the above equation is

$$\begin{aligned}\sum_{k=0}^{n-1}\left(x + \frac{k}{n} - \left\lfloor x + \frac{k}{n} \right\rfloor - \frac{1}{2}\right) &= nx + \frac{1}{n}\sum_{k=0}^{n-1} k - \sum_{k=0}^{n-1}\left\lfloor x + \frac{k}{n} \right\rfloor - \frac{1}{2}n \\ &= nx + \frac{n-1}{2} - \lfloor nx \rfloor - \frac{n}{2} \\ &= nx - \lfloor nx \rfloor - \frac{1}{2} = f(nx). \qquad \square\end{aligned}$$

**Example 3.15.** Let $n \in \mathbb{N}$. Show that

$$n = \left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{2^2} \right\rfloor + \left\lfloor \frac{n+2^2}{2^3} \right\rfloor + \left\lfloor \frac{n+2^3}{2^4} \right\rfloor + \cdots.$$

**Solution.** When $k$ is large enough, the term $\left\lfloor \frac{n+2^k}{2^{k+1}} \right\rfloor = \left\lfloor \frac{1}{2} + \frac{n}{2^{k+1}} \right\rfloor = 0$, so the right-hand side of the above equation is actually a finite sum.

Applying Hermite's identity in the form $\left\lfloor x+\frac{1}{2}\right\rfloor = \lfloor 2x\rfloor - \lfloor x\rfloor$, the right-hand side of the above equation is equal to

$$\begin{aligned}&\left\lfloor\frac{1}{2}+\frac{n}{2}\right\rfloor+\left\lfloor\frac{1}{2}+\frac{n}{2^2}\right\rfloor+\left\lfloor\frac{1}{2}+\frac{n}{2^3}\right\rfloor+\left\lfloor\frac{1}{2}+\frac{n}{2^4}\right\rfloor+\cdots\\ &\quad=n-\left\lfloor\frac{n}{2}\right\rfloor+\left\lfloor\frac{n}{2}\right\rfloor-\left\lfloor\frac{n}{2^2}\right\rfloor+\left\lfloor\frac{n}{2^2}\right\rfloor-\left\lfloor\frac{n}{2^3}\right\rfloor+\left\lfloor\frac{n}{2^3}\right\rfloor-\left\lfloor\frac{n}{2^4}\right\rfloor+\cdots,\end{aligned}$$

which telescopes and is equal to $n$. □

**Example 3.16.** Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Determine the sum

$$\sum_{0\le i<j\le n}\left\lfloor\frac{x+i}{j}\right\rfloor.$$

**Solution.** We rewrite the above as a double sum and evaluate it by using Hermite's identity. We have

$$\sum_{j=1}^{n}\sum_{i=0}^{j-1}\left\lfloor\frac{x}{j}+\frac{i}{j}\right\rfloor=\sum_{j=1}^{n}\left\lfloor j\frac{x}{j}\right\rfloor=n\lfloor x\rfloor. \qquad \square$$

Finally, we record our observation concerning the sum of the floor function as follows.

**Theorem 3.17.** *Suppose that $a, m \in \mathbb{N}$, $a \ge 3$, $a$ is odd, $a^d \parallel m$, $q = \frac{m}{a^d}$, and $r = q \bmod a$ is the remainder in the division of $q$ by $a$. Then*

$$\sum_{k=0}^{m}\sum_{\ell=1}^{\frac{a-1}{2}}\left(\left\lfloor\frac{\ell a^k+m}{a^{k+1}}\right\rfloor-\left\lfloor\frac{\ell a^k-m}{a^{k+1}}\right\rfloor\right) = \begin{cases} m-1, & \textit{if } 1\le r\le \frac{a-1}{2};\\ m, & \textit{if } \frac{a+1}{2}\le r\le a-1.\end{cases} \tag{3.6}$$

**Proof. Case 1** $a \nmid m$. That is $d = 0$ and $q = m$. If $k \ge 1$ and $\frac{\ell a^k \pm m}{a^{k+1}} \in \mathbb{Z}$, then $\ell a^k \pm m \equiv 0 \pmod{a^k}$, which implies $m \equiv 0 \pmod a$, a contradiction. So $\frac{\ell a^k \pm m}{a^{k+1}}$ is not an integer for any $k \ge 1$. Recall that $\lfloor -x\rfloor = -\lfloor x\rfloor - 1$ for $x \notin \mathbb{Z}$. Therefore, for $k \ge 1$, we have

$$\left\lfloor\frac{\ell a^k+m}{a^{k+1}}\right\rfloor-\left\lfloor\frac{\ell a^k-m}{a^{k+1}}\right\rfloor=\left\lfloor\frac{m}{a^{k+1}}+\frac{\ell}{a}\right\rfloor+\left\lfloor\frac{m}{a^{k+1}}-\frac{\ell}{a}\right\rfloor+1.$$

Let $k \ge 1$ and $x = \frac{m}{a^{k+1}} - \frac{\frac{a-1}{2}}{a}$. Then the inner sum on the left-hand side of (3.6) can be written in a form suitable for an application of Hermite's identity as

$$\sum_{\ell=1}^{\frac{a-1}{2}}\left(\left\lfloor\frac{m}{a^{k+1}}+\frac{\ell}{a}\right\rfloor+\left\lfloor\frac{m}{a^{k+1}}-\frac{\ell}{a}\right\rfloor+1\right)=\frac{a-1}{2}+\sum_{\substack{0\le b\le a-1\\ b\neq\frac{a-1}{2}}}\left\lfloor x+\frac{b}{a}\right\rfloor$$

$$=\frac{a-1}{2}+\lfloor ax\rfloor-\left\lfloor x+\frac{a-1}{2a}\right\rfloor=\left\lfloor\frac{m}{a^k}\right\rfloor-\left\lfloor\frac{m}{a^{k+1}}\right\rfloor.$$

Separating the sum when $k=0$ and $1\le k\le m$, the left-hand side of (3.6) is

$$\sum_{\ell=1}^{\frac{a-1}{2}}\left(\left\lfloor\frac{\ell+m}{a}\right\rfloor-\left\lfloor\frac{\ell-m}{a}\right\rfloor\right)+\sum_{k=1}^{m}\left(\left\lfloor\frac{m}{a^k}\right\rfloor-\left\lfloor\frac{m}{a^{k+1}}\right\rfloor\right). \tag{3.7}$$

Since $a^{m+1}>m$ and $r=q \bmod a=m \bmod a$, we see that the second sum in (3.7) telescopes and is equal to

$$\left\lfloor\frac{m}{a}\right\rfloor-\left\lfloor\frac{m}{a^{m+1}}\right\rfloor=\left\lfloor\frac{m}{a}\right\rfloor=\left\lfloor\frac{m-r}{a}+\frac{r}{a}\right\rfloor=\frac{m-r}{a}.$$

Similarly,

$$\left\lfloor\frac{\ell+m}{a}\right\rfloor=\left\lfloor\frac{m-r}{a}+\frac{\ell+r}{a}\right\rfloor=\frac{m-r}{a}+\left\lfloor\frac{\ell+r}{a}\right\rfloor,$$
$$\left\lfloor\frac{\ell-m}{a}\right\rfloor=\left\lfloor\frac{-m+r}{a}+\frac{\ell-r}{a}\right\rfloor=\frac{-m+r}{a}+\left\lfloor\frac{\ell-r}{a}\right\rfloor,$$

and the first sum in (3.7) is

$$\frac{2(m-r)}{a}\left(\frac{a-1}{2}\right)+\sum_{\ell=1}^{\frac{a-1}{2}}\left(\left\lfloor\frac{\ell+r}{a}\right\rfloor-\left\lfloor\frac{\ell-r}{a}\right\rfloor\right).$$

Combining the first and second sums, (3.7) becomes

$$m-r+\sum_{\ell=1}^{\frac{a-1}{2}}\left(\left\lfloor\frac{\ell+r}{a}\right\rfloor-\left\lfloor\frac{\ell-r}{a}\right\rfloor\right). \tag{3.8}$$

Let $1\le\ell\le\frac{a-1}{2}$. Then $1\le\ell+r\le\frac{a-1}{2}+a-1<2a$, so $\left\lfloor\frac{\ell+r}{a}\right\rfloor=0$ or $1$. Similarly, $-a<\ell-r<a$, so $\left\lfloor\frac{\ell-r}{a}\right\rfloor=0$ or $-1$. Moreover, we have

$$\left\lfloor\frac{\ell+r}{a}\right\rfloor=1 \quad\text{if and only if}\quad \ell\ge a-r; \tag{3.9}$$

$$\left\lfloor\frac{\ell-r}{a}\right\rfloor=-1 \quad\text{if and only if}\quad \ell<r. \tag{3.10}$$

**Case 1.1** $r \geq \frac{a+1}{2}$. The condition $\ell < r$ in (3.10) is satisfied by all $\ell = 1, 2, \ldots, \frac{a-1}{2}$. In addition, $1 \leq a - r \leq \frac{a-1}{2}$. Therefore, by (3.9) and (3.10), the sum in (3.8) is equal to

$$\sum_{1 \leq \ell \leq \frac{a-1}{2}} \left\lfloor \frac{\ell + r}{a} \right\rfloor - \sum_{1 \leq \ell \leq \frac{a-1}{2}} \left\lfloor \frac{\ell - r}{a} \right\rfloor = \sum_{a - r \leq \ell \leq \frac{a-1}{2}} 1 + \sum_{1 \leq \ell \leq \frac{a-1}{2}} 1 = r.$$

Hence (3.8) is equal to $m - r + r = m$.

**Case 1.2** $1 \leq r \leq \frac{a-1}{2}$. Then the condition $\ell \geq a - r$ in (3.9) is always false. So the sum $\sum_{\ell=1}^{\frac{a-1}{2}} \left\lfloor \frac{\ell + r}{a} \right\rfloor = 0$ and (3.8) is equal to

$$m - r - \sum_{\ell=1}^{\frac{a-1}{2}} \left\lfloor \frac{\ell - r}{a} \right\rfloor = m - r + \sum_{1 \leq \ell < r} 1 = m - r + r - 1 = m - 1.$$

This completes the proof in the case $a \nmid m$.

**Case 2** $a \mid m$. Since $a^d \mid m$, we see that for $0 \leq k \leq d-1$ and $1 \leq \ell \leq \frac{a-1}{2}$,

$$\left\lfloor \frac{\ell a^k \pm m}{a^{k+1}} \right\rfloor = \left\lfloor \frac{\pm m}{a^{k+1}} + \frac{\ell}{a} \right\rfloor = \frac{\pm m}{a^{k+1}}.$$

Recall also that $m = qa^d$. So the left-hand side of (3.6) is equal to

$$\sum_{k=0}^{d-1} \sum_{\ell=1}^{\frac{a-1}{2}} \frac{2m}{a^{k+1}} + \sum_{k=d}^{m} \sum_{\ell=1}^{\frac{a-1}{2}} \left\lfloor \frac{\ell}{a} + \frac{qa^d}{a^{k+1}} \right\rfloor - \left\lfloor \frac{\ell}{a} - \frac{qa^d}{a^{k+1}} \right\rfloor$$

$$= m\left(1 - \frac{1}{a^d}\right) + \sum_{k=0}^{m-d} \sum_{\ell=1}^{\frac{a-1}{2}} \left\lfloor \frac{\ell}{a} + \frac{q}{a^{k+1}} \right\rfloor - \left\lfloor \frac{\ell}{a} - \frac{q}{a^{k+1}} \right\rfloor. \tag{3.11}$$

Since $a \geq 3$ and $d \geq 1$, we have $a^d \geq d + 2$, which can be proved by induction on $d$. We observe that

$$m - d - q = (a^d - 1)q - d \geq a^d - 1 - d \geq 1.$$

So $q + 1 \leq m - d$, and therefore we can divide the sum over $k = 0, 1, 2, \ldots, m - d$ in (3.11) into two parts: $S_1$ and $S_2$ where $S_1$ and $S_2$ are, respectively, the sum over $k = 0, 1, \ldots, q$ and $k = q + 1, \ldots, m - d$. Since $a^d \parallel m$ and $q = \frac{m}{a^d}$, we have $a \nmid q$ and $S_1$ can be evaluated by the result in Case 1. We obtain

$$S_1 = \begin{cases} q - 1, & \text{if } 1 \leq r \leq \frac{a-1}{2}; \\ q, & \text{if } \frac{a+1}{2} \leq r \leq a - 1. \end{cases}$$

Next, let $q+1 \le k \le m-d$. We observe that $a^{q+1} > q$. Therefore

$$0 \le \frac{\ell}{a} + \frac{q}{a^{k+1}} \le \frac{a-1}{2a} + \frac{q}{a^{q+2}} < \frac{1}{2} - \frac{1}{2a} + \frac{1}{a} < \frac{1}{2} + \frac{1}{3} < 1,$$
$$0 < \frac{1}{a} - \frac{q}{a^{q+2}} \le \frac{\ell}{a} - \frac{q}{a^{k+1}} \le \frac{\ell}{a} \le \frac{a-1}{2a} < \frac{1}{2}.$$

These imply $\left\lfloor \frac{\ell}{a} + \frac{q}{a^{k+1}} \right\rfloor = \left\lfloor \frac{\ell}{a} - \frac{q}{a^{k+1}} \right\rfloor = 0$ and thus $S_2 = 0$. Recalling that (3.11) is equal to $m\left(1 - \frac{1}{a^d}\right) + S_1 + S_2 = m - q + S_1$, we obtain the desired result. □

## 3.3. Counting Lattice Points

Recall that a point $(x, y) \in \mathbb{R}^2$ is called a *lattice point* if both $x$ and $y$ are integers. One of the many proofs of the quadratic reciprocity law involves the use of the floor function in counting lattice points on the plane. This includes the proof given by Gauss [**141**] and Eisenstein [**109**]. See also the discussion on Gauss and Eisenstein's proof in [**241**, **242**, **375**]. The method is useful not only in proving the quadratic reciprocity law but also in deriving summation formulas involving the floor function. We present such formulas in this section. We remark that many of our formulas in this section are new.

First, let us consider this problem on the real line. Let $x, y \in \mathbb{R}$ and $x < y$. If $x, y \in \mathbb{Z}$, it is easy to see that the number of integers contained in the intervals $[x, y]$, $[x, y)$, $(x, y]$, $(x, y)$ are given by

$$|\mathbb{Z} \cap [x, y]| = y - x + 1,$$
$$|\mathbb{Z} \cap [x, y)| = y - x,$$
$$|\mathbb{Z} \cap (x, y]| = y - x,$$
$$|\mathbb{Z} \cap (x, y)| = y - x - 1.$$

When $x$ or $y$ is not an integer, the counting is a bit more complicated. For example, if $x \notin \mathbb{Z}$ and $y \in \mathbb{Z}$, then

$$|\mathbb{Z} \cap [x, y]| = |\mathbb{Z} \cap [\lceil x \rceil, y]| = y - \lceil x \rceil + 1.$$

In general, for each $x, y \in \mathbb{R}$ with $x < y$, we have

$$|\mathbb{Z} \cap [x,y]| = \lfloor y \rfloor - \lceil x \rceil + 1, \tag{3.12}$$

$$|\mathbb{Z} \cap [x,y)| = \lceil y \rceil - \lceil x \rceil, \tag{3.13}$$

$$|\mathbb{Z} \cap (x,y]| = \lfloor y \rfloor - \lfloor x \rfloor, \tag{3.14}$$

$$|\mathbb{Z} \cap (x,y)| = \lceil y \rceil - \lfloor x \rfloor - 1. \tag{3.15}$$

The formulas (3.12), (3.13), and (3.14) also hold when $x = y$ but (3.15) does not hold when $x = y$ and $x \in \mathbb{Z}$ since the left-hand side will be zero while the right-hand side is $-1$. The verification can be done by considering them case by case and is left as an exercise to the reader. We will use these formulas in the subsequent counting without further reference. The proof of the next theorem is adapted from Andreescu and Andrica [**8**].

**Theorem 3.18.** *Let a, b, c, d be nonnegative real numbers and let* $f : [a,b] \to [c,d]$ *be a bijective, increasing, and continuous function. Let* $G_f \subseteq \mathbb{R}^2$ *be the graph of* $f$. *Then*

$$\sum_{a \le k \le b} \lfloor f(k) \rfloor + \sum_{c \le k \le d} \lfloor f^{-1}(k) \rfloor - |\mathbb{Z}^2 \cap G_f| = \lfloor b \rfloor \lfloor d \rfloor - \lceil a-1 \rceil \lceil c-1 \rceil,$$

*where* $|\mathbb{Z}^2 \cap G_f|$ *is the number of lattice points on the graph of* $f$.

**Proof.** Since $f$ is continuous, we can consider the following regions:

$$M_1 = \{(x,y) \in \mathbb{R}^2 \mid a \le x \le b \text{ and } 0 \le y \le f(x)\},$$
$$M_2 = \{(x,y) \in \mathbb{R}^2 \mid c \le y \le d \text{ and } 0 \le x \le f^{-1}(y)\},$$
$$M_3 = \{(x,y) \in \mathbb{R}^2 \mid 0 \le x \le b \text{ and } 0 \le y \le d\},$$
$$M_4 = \{(x,y) \in \mathbb{R}^2 \mid 0 \le x < a \text{ and } 0 \le y < c\}.$$

For convenience, let $|A^*|$ be the number of lattice points in the set $A$. We first count $|M_1^*|$. For each fix $x \in [a,b] \cap \mathbb{Z}$, the number of $y \in \mathbb{Z}$ such that $(x,y) \in M_1^*$ is equal to

$$|\mathbb{Z} \cap [0, f(x)]| = \lfloor f(x) \rfloor + 1.$$

Therefore the number of lattice points in $M_1$ is given by

$$|M_1^*| = \sum_{a \le k \le b} (\lfloor f(k) \rfloor + 1).$$

Similarly,

$$\begin{aligned}
|M_2^*| &= \sum_{c\le y\le d} |\mathbb{Z}\cap[0,f^{-1}(y)]| = \sum_{c\le k\le d} \left(\lfloor f^{-1}(k)\rfloor + 1\right),\\
|M_3^*| &= |\mathbb{Z}\cap[0,b]|\cdot|\mathbb{Z}\cap[0,d]| = (\lfloor b\rfloor+1)(\lfloor d\rfloor+1),\\
|M_4^*| &= |\mathbb{Z}\cap[0,a)|\cdot|\mathbb{Z}\cap[0,c)| = \lceil a\rceil\cdot\lceil c\rceil.
\end{aligned}$$

Since $M_1 \cup M_2 = M_3 - M_4$ and $M_1 \cap M_2 = G_f$, we obtain that

$$|M_1^*| + |M_2^*| - |M_1^*\cap M_2^*| = |M_1^*\cup M_2^*| = |M_3^* - M_4^*| = |M_3^*| - |M_4^*|,$$

which leads to the identity

$$\begin{aligned}
\sum_{a\le k\le b} (\lfloor f(k)\rfloor + 1) + \sum_{c\le k\le d} \left(\lfloor f^{-1}(k)\rfloor + 1\right) - |\mathbb{Z}^2\cap G_f|&\\
= (\lfloor b\rfloor+1)(\lfloor d\rfloor+1) - \lceil a\rceil\cdot\lceil c\rceil&.
\end{aligned} \tag{3.16}$$

The left-hand side of (3.16) is

$$\begin{aligned}
&\sum_{a\le k\le b} \lfloor f(k)\rfloor + \sum_{c\le k\le d} \lfloor f^{-1}(k)\rfloor - |\mathbb{Z}^2\cap G_f| + |\mathbb{Z}\cap[a,b]| + |\mathbb{Z}\cap[c,d]|\\
&= \sum_{a\le k\le b} \lfloor f(k)\rfloor + \sum_{c\le k\le d} \lfloor f^{-1}(k)\rfloor - |\mathbb{Z}^2\cap G_f| + \lfloor b\rfloor - \lceil a\rceil + 1 + \lfloor d\rfloor - \lceil c\rceil + 1.
\end{aligned}$$

After canceling $\lfloor b\rfloor - \lceil a\rceil + 1 + \lfloor d\rfloor - \lceil c\rceil + 1$ on both sides of (3.16), we obtain the desired result. ☐

By choosing different regions, we can obtain a different version of Theorem 3.18 where the graph of $f$ does not appear in the equation.

**Theorem 3.19.** *Let a, b, c, d, and f be as in Theorem* 3.18. *Then*

$$\sum_{a\le k\le b} \lfloor f(k)\rfloor + \sum_{c\le k\le d} \lceil f^{-1}(k)\rceil = \lfloor d\rfloor\lfloor b+1\rfloor - \lceil c-1\rceil\lceil a\rceil.$$

**Proof.** The proof is similar to that of Theorem 3.18 but we choose the sets differently as follows:

$$\begin{aligned}
M_1 &= \{(x,y)\in\mathbb{Z}^2 \mid a\le x\le b \text{ and } c\le y\le f(x)\},\\
M_2 &= \{(x,y)\in\mathbb{Z}^2 \mid c\le y\le d \text{ and } f^{-1}(y)\le x\le b\} = M_1,\\
M_3 &= \{(x,y)\in\mathbb{Z}^2 \mid a\le x\le b \text{ and } 0\le y< c\}.
\end{aligned}$$

We use $(x, y) \in \mathbb{Z}^2$ in the definitions of $M_1$, $M_2$, and $M_3$ so that they are sets of lattice points. We have $M_2 \cap M_3 = \emptyset$ and

$$\begin{aligned} |M_2 \cup M_3| &= |M_2| + |M_3| \\ &= \sum_{c \le k \le d} |\mathbb{Z} \cap [f^{-1}(k), b]| + (\lfloor b \rfloor - \lceil a \rceil + 1)\lceil c \rceil \\ &= \sum_{c \le k \le d} \left(\lfloor b \rfloor - \left\lceil f^{-1}(k) \right\rceil + 1\right) + (\lfloor b \rfloor - \lceil a \rceil + 1)\lceil c \rceil . \end{aligned} \tag{3.17}$$

On the other hand, we have

$$M_2 \cup M_3 = M_1 \cup M_3 = \{(x, y) \in \mathbb{Z}^2 \mid a \le x \le b, 0 \le y \le f(x)\},$$

and so

$$|M_2 \cup M_3| = \sum_{a \le k \le b} |\mathbb{Z} \cap [0, f(k)]| = \sum_{a \le k \le b} (\lfloor f(k) \rfloor + 1) . \tag{3.18}$$

By putting (3.17) and (3.18) together, we obtain the desired result. ☐

We can also obtain the corresponding results for decreasing functions as given in the next theorem.

**Theorem 3.20.** *Let $a$, $b$, $c$, $d$ be nonnegative real numbers and let $f : [a, b] \to [c, d]$ be bijective, decreasing, and continuous. Then*

$$\sum_{a \le k \le b} \lfloor f(k) \rfloor - \sum_{c \le k \le d} \left\lfloor f^{-1}(k) \right\rfloor = \lfloor b \rfloor \lceil c - 1 \rceil - \lfloor d \rfloor \lceil a - 1 \rceil .$$

**Proof.** The proof is similar to that of Theorem 3.19. We consider the following sets:

$$\begin{aligned} M_1 &= \{(x, y) \in \mathbb{Z}^2 \mid a \le x \le b \text{ and } c \le y \le f(x)\}, \\ M_2 &= \{(x, y) \in \mathbb{Z}^2 \mid c \le y \le d \text{ and } a \le x \le f^{-1}(y)\} = M_1, \\ M_3 &= \{(x, y) \in \mathbb{Z}^2 \mid a \le x \le b \text{ and } 0 \le y < c\}, \\ M_4 &= \{(x, y) \in \mathbb{Z}^2 \mid 0 \le x < a \text{ and } c \le y \le d\}. \end{aligned}$$

Then $M_1 \cap M_3 = \emptyset$, $M_2 \cap M_4 = \emptyset$, and we obtain

$$\begin{aligned} |M_1| + |M_3| &= |M_1 \cup M_3| = \sum_{a \le k \le b} (\lfloor f(k) \rfloor + 1) , \\ |M_2| + |M_4| &= |M_2 \cup M_4| = \sum_{c \le k \le d} \left(\left\lfloor f^{-1}(k) \right\rfloor + 1\right) , \end{aligned}$$

$$|M_3| = (\lfloor b \rfloor - \lceil a \rceil + 1)\lceil c \rceil , \quad |M_4| = \lceil a \rceil (\lfloor d \rfloor - \lceil c \rceil + 1).$$

The above leads to

$$\sum_{a\le k\le b} \lfloor f(k)\rfloor - \sum_{c\le k\le d} \left\lfloor f^{-1}(k)\right\rfloor = \lfloor b\rfloor \lceil c-1\rceil - \lfloor d\rfloor \lceil a-1\rceil ,$$

as desired. ☐

Similar to Theorems 3.18 and 3.19, a different choice of regions leads to another version of the equation.

**Theorem 3.21.** *Let a, b, c, d, and f be as in Theorem* 3.20. *Then*

$$\sum_{a\le k\le b} \lfloor f(k)\rfloor - \sum_{c\le k\le d} \left\lceil f^{-1}(k)\right\rceil - |\mathbb{Z}^2 \cap G_f| = \lfloor b+1\rfloor \lceil c-1\rceil - \lceil a\rceil \lfloor d\rfloor ,$$

*where* $|\mathbb{Z}^2 \cap G_f|$ *is the number of the lattice points on the graph of* $f$.

**Proof.** We consider the following sets:

$$\begin{aligned} M_1 &= \{(x,y)\in \mathbb{Z}^2 \mid a\le x\le b \text{ and } 0\le y\le f(x)\},\\ M_2 &= \{(x,y)\in \mathbb{Z}^2 \mid c\le y\le d \text{ and } f^{-1}(y)\le x\le b\},\\ M_3 &= \{(x,y)\in \mathbb{Z}^2 \mid 0\le x\le b \text{ and } 0\le y\le d\},\\ M_4 &= \{(x,y)\in \mathbb{Z}^2 \mid 0\le x< a \text{ and } 0\le y\le d\}. \end{aligned}$$

Then $M_1 \cup M_2 = M_3 - M_4$ and the equation

$$|M_3| - |M_4| = |M_3 - M_4| = |M_1 \cup M_2| = |M_1| + |M_2| - |G_f|$$

leads to the desired formula. We leave the details to the reader. ☐

**Remark 3.22.** There may be other different versions of Theorems 3.18, 3.19, 3.20, and 3.21, some of which may be equivalent. We leave this to the reader's imagination. Nevertheless, these theorems lead to some important well-known results as shown below.

**Theorem 3.23.** *Let m, n, s be positive integers and let* $m\le n$. *Then*

$$\sum_{k=1}^{s} \left\lfloor \frac{km}{n}\right\rfloor + \sum_{1\le k\le \frac{ms}{n}} \left\lfloor \frac{kn}{m}\right\rfloor = s\left\lfloor \frac{ms}{n}\right\rfloor + \left\lfloor \frac{s\gcd(m,n)}{n}\right\rfloor .$$

**Proof.** Let $f : [1,s] \to \left[\frac{m}{n}, \frac{sm}{n}\right]$ be given by $f(x) = \frac{m}{n}x$. By Theorem 3.18, it only remains to show that

$$|\mathbb{Z}^2 \cap G_f| = \left\lfloor \frac{s\gcd(m,n)}{n}\right\rfloor .$$

We have

$$\mathbb{Z}^2 \cap G_f \subseteq \left\{\left(1, \frac{m}{n}\right), \left(2, \frac{2m}{n}\right), \dots, \left(s, \frac{sm}{n}\right)\right\} \quad \text{and}$$
$$|\mathbb{Z}^2 \cap G_f| = \left|\mathbb{Z} \cap \left\{\frac{m}{n}, \frac{2m}{n}, \dots, \frac{sm}{n}\right\}\right|.$$

Let $d = \gcd(m, n)$. Then $\frac{m}{n} = \frac{m_1}{n_1}$ where $m_1 = \frac{m}{d}$, $n_1 = \frac{n}{d}$, and $(m_1, n_1) = 1$. Then

$$\left\{\frac{m}{n}, \frac{2m}{n}, \dots, \frac{sm}{n}\right\} = \left\{\frac{m_1}{n_1}, \frac{2m_1}{n_1}, \dots, \frac{sm_1}{n_1}\right\}, \text{ and}$$
$$\left|\mathbb{Z} \cap \left\{\frac{m}{n}, \frac{2m}{n}, \dots, \frac{sm}{n}\right\}\right| = \sum_{\substack{1 \le k \le s \\ n_1 | k}} 1 = \left\lfloor \frac{s}{n_1} \right\rfloor = \left\lfloor \frac{sd}{n} \right\rfloor,$$

as required. This completes the proof. ☐

**Corollary 3.24.** *For $m, n \in \mathbb{N}$, we have*

$$\sum_{k=1}^{n} \left\lfloor \frac{km}{n} \right\rfloor + \sum_{k=1}^{m} \left\lfloor \frac{kn}{m} \right\rfloor = mn + \gcd(m, n).$$

**Proof.** Since both sides of the equation are symmetric in $m$ and $n$, we can assume that $m \le n$. Then by the substitution $s = n$ in Theorem 3.23, we obtain the desired result. ☐

There are some formulas that look similar to those given in Theorem 3.23 and they can be proved by using our theorem as shown in the next example.

**Example 3.25.** The following are identities appearing in Murray's thesis [**279**, pages 16, 26, 49–51, 54].

(i) Let $n \in \mathbb{N}$, $a \in \mathbb{R}$, $a > 1$, and $m = \lfloor a^n \rfloor$. Then

$$\sum_{k=1}^{n} \lfloor a^k \rfloor + \sum_{k=1}^{m} \left\lfloor \frac{\log k}{\log a} \right\rfloor = \begin{cases} (m+1)n, & \text{if } a \in \mathbb{Z}; \\ mn, & \text{if } a \in \mathbb{Q} \setminus \mathbb{Z} \text{ or} \\ & \ a \text{ is transcendental.} \end{cases}$$

The condition $a \in \mathbb{Q} \setminus \mathbb{Z}$ or $a$ is transcendental may be replaced by a statement such as $a$ is not an algebraic integer. The point is that, in this case, $a^k \notin \mathbb{Z}$ for any $k \ge 1$.

(ii) If $\alpha$ is a positive irrational number and $n \in \mathbb{N}$, then

$$\sum_{k=0}^{n} \lfloor k\alpha \rfloor + \sum_{k=0}^{\lfloor nx \rfloor} \left\lfloor \frac{k}{\alpha} \right\rfloor = n \lfloor n\alpha \rfloor \tag{3.19}$$

$$\sum_{k=0}^{n} \lfloor k\alpha \rfloor - \sum_{k=0}^{\lfloor n\alpha \rfloor} \left\lfloor -\frac{k}{\alpha} \right\rfloor = (n+1) \lfloor n\alpha \rfloor . \tag{3.20}$$

In fact, Murray claimed that (i) holds for all $a \in \mathbb{R} \cap (1, \infty)$, which is incorrect. For instance, when $a = \sqrt{2}$ and $n = 4$, the left-hand side of the equation is 18 while $mn = 16$ and $(m+1)n = 20$. Nevertheless, the identities 4.5 and 4.6 in [**279**, p. 16], which Murray quoted from Hacks [**165**], is correct since, in these cases, $a = 10$ which is integral or $a = e$ which is transcendental.

**Solution.** Let $f : [1, n] \to [a, a^n]$ be given by $f(x) = a^x$. Then by Theorem 3.18, we obtain

$$\sum_{k=1}^{n} \lfloor a^k \rfloor + \sum_{a \le k \le a^k} \left\lfloor \frac{\log k}{\log a} \right\rfloor - |\mathbb{Z}^2 \cap G_f| = mn.$$

If $1 \le k < a$, then $\left\lfloor \frac{\log k}{\log a} \right\rfloor = 0$, so the second sum on the left-hand side above can be taken over $k \in [1, m]$. So it only remains to count the number of the lattice points on the graph of $f$. If $a \in \mathbb{Z}$, then obviously $(1, a), (2, a^2), \ldots, (n, a^n)$ are the lattice points and so $|\mathbb{Z}^2 \cap G_f| = n$. If $a$ is transcendental or $a \in \mathbb{Q} \setminus \mathbb{Z}$, then there is no lattice point in $G_f$. This implies (i). Similarly, (3.19) follows by applying Theorem 3.18 to the function $f : [0, n] \to [0, n\alpha]$ given by $f(x) = \alpha x$. Furthermore, $\left\lfloor -\frac{k}{\alpha} \right\rfloor = -\left\lceil \frac{k}{\alpha} \right\rceil$ for all $k \ge 1$, by Theorem 3.3(v). Therefore (3.20) follows by applying Theorem 3.19 to the same function. This completes the proof. □

## 3.4. Miscellaneous Examples

In this section, we present various calculations involving the floor function. We begin with sums that have some kind of symmetric property.

**Example 3.26.** (Gauss) Let $a$ and $b$ be relatively prime positive integers. Then

$$\sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = \frac{(a-1)(b-1)}{2}.$$

**Solution.** Replacing $k$ by $b-k$, the sum is not changed. Therefore

$$\sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = \sum_{k=1}^{b-1} \left\lfloor \frac{(b-k)a}{b} \right\rfloor = \sum_{k=1}^{b-1} \left( a + \left\lfloor \frac{-ka}{b} \right\rfloor \right).$$

Recall that $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$ for $x \notin \mathbb{Z}$, so the above becomes

$$\sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = (b-1)a - \sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor - (b-1),$$

which leads the desired formula. ☐

**Example 3.27.** (Landau) Suppose $a$ and $b$ are odd and are relatively prime positive integers. Then

$$\sum_{k=1}^{\frac{b-1}{2}} \left\lfloor \frac{ka}{b} \right\rfloor + \sum_{k=1}^{\frac{a-1}{2}} \left\lfloor \frac{kb}{a} \right\rfloor = \frac{(a-1)(b-1)}{4}.$$

**Solution.** By applying Theorem 3.18 to the function $f : \left[1, \frac{b}{2}\right] \to \left[\frac{a}{b}, \frac{a}{2}\right]$ given by $f(x) = \frac{a}{b}x$, we obtain

$$\sum_{1 \le k \le \frac{b}{2}} \left\lfloor \frac{ka}{b} \right\rfloor + \sum_{\frac{a}{b} \le k \le \frac{a}{2}} \left\lfloor \frac{kb}{a} \right\rfloor = \frac{(a-1)(b-1)}{4}.$$

Since $a$ and $b$ are odd, the conditions $k \le \frac{b}{2}$ and $k \le \frac{a}{2}$ are the same as $k \le \frac{b-1}{2}$ and $k \le \frac{a-1}{2}$. In addition, if $a < b$, the condition $a/b \le k \le (a-1)/2$ is equivalent to $1 \le k \le (a-1)/2$. Furthermore if $a \ge b$ and $1 \le k < a/b$, then $\lfloor kb/a \rfloor = 0$, and so

$$\sum_{\frac{a}{b} \le k \le \frac{a}{2}} \left\lfloor \frac{kb}{a} \right\rfloor = \sum_{1 \le k \le \frac{a-1}{2}} \left\lfloor \frac{kb}{a} \right\rfloor.$$

This completes the proof. (The sums similar to Examples 3.26 and 3.27 are also given in the exercise.) ☐

The floor function is also used to express the number of digits in the $b$-adic representation of integers.

**Example 3.28.** Let $\log_b x$ be the base $b$ logarithmic function of a positive real number $x$. If $n \in \mathbb{N}$, show that $\lfloor \log_b n \rfloor + 1$ is the length of the $b$-adic expansion of $n$. In other words, if $n = (a_k a_{k-1} \cdots a_0)_b$ is the expansion of $n$ in base $b$ with $a_k \neq 0$, then $k = \left\lfloor \frac{\log n}{\log b} \right\rfloor$.

**Solution.** $n \geq a_k b^k \geq b^k$ and $n < b^{k+1}$. So $k$ is the largest integer such that $b^k \leq n$, or $k \leq \frac{\log n}{\log b}$. So $k = \left\lfloor \frac{\log n}{\log b} \right\rfloor$. ☐

In Examples 3.29 to 3.33, we collect some interesting results from exercises and exams in some mathematical competitions.

**Example 3.29.** Find a closed form of $\sum_{k=1}^{n} \lfloor \sqrt{k} \rfloor$ in terms of $n$ and $a = \lfloor \sqrt{n} \rfloor$.

**Solution.** We observe that

$$\lfloor \sqrt{k} \rfloor = m \text{ if and only if } m^2 \leq k < (m+1)^2.$$

So we write the sum in question as

$$\begin{aligned}
&\sum_{1 \leq m \leq \sqrt{n}-1} \; \sum_{m^2 \leq k < (m+1)^2} \lfloor \sqrt{k} \rfloor + \sum_{\lfloor \sqrt{n} \rfloor^2 \leq k \leq n} \lfloor \sqrt{k} \rfloor \\
&= \sum_{1 \leq m \leq a-1} \; \sum_{m^2 \leq k < (m+1)^2} m + \sum_{a^2 \leq k \leq n} \lfloor \sqrt{k} \rfloor \\
&= \sum_{1 \leq m \leq a-1} m(2m+1) + (n - a^2 + 1)a \\
&= \frac{a(a-1)(4a+1)}{6} + (n - a^2 + 1)a \\
&= (n+1)a - \frac{a(a+1)(2a+1)}{6}.
\end{aligned}$$

**Alternative Solution.** We can apply Theorem 3.18 to the function $f(x) = \sqrt{x}$ to obtain the desired formula. ☐

**Example 3.30.** Determine all positive integers $n$ such that $\lfloor \sqrt{n} \rfloor$ divides $n$.

**Solution.** Suppose that $n \in \mathbb{N}$ and $\lfloor \sqrt{n} \rfloor$ divides $n$. Then there is $m \geq 1$ such that $m^2 \leq n < (m+1)^2$. Then $m \leq \sqrt{n} < m+1$ and so $\lfloor \sqrt{n} \rfloor = m$. The integers that are larger than or equal to $m^2$ and are divisible by $m$ are of the form $m^2 + km$ where $k \geq 0$. Since $m^2 + 3m > (m+1)^2$, the integers in $[m^2, (m+1)^2)$ that are divisible by $m$ are $m^2$, $m^2+m$, and $m^2+2m$. It is easy to check the converse: if $n = m^2, m^2+m, m^2+2m$ for some $m \in \mathbb{N}$, then $\lfloor \sqrt{n} \rfloor$ divides $n$. Therefore $\lfloor \sqrt{n} \rfloor$ divides $n$ if and only if $n = m^2, m^2+m, m^2+2m$ for some $m \in \mathbb{N}$. A few terms of such $n$ are $n = 1, 2, 3, 4, 6, 8, 9, 12, 15$ (corresponding to $m = 1, 2, 3$). $\square$

A sum involving the fractional parts such as $\sum_{n \le x} \{x/n\}$ is generally difficult to estimate, but there are some sums that are simple enough to be an exercise as shown in Examples 3.31 and 3.32.

**Example 3.31.** (1999 Russian Mathematical Olympiad) Prove that for every natural number $n$,

$$\sum_{k=1}^{n^2} \{\sqrt{k}\} < \frac{n^2-1}{2}.$$

**Solution.** Since $\{\sqrt{k}\} = 0$ if $k$ is a square, the sum in question is equal to

$$\sum_{m=1}^{n-1} \sum_{m^2<k<(m+1)^2} \{\sqrt{k}\} = \sum_{m=1}^{n-1} \sum_{m^2<k<(m+1)^2} (\sqrt{k} - m).$$

For $m^2 < k < (m+1)^2$, we have $\sqrt{k} - m = \frac{k-m^2}{\sqrt{k}+m} < \frac{k-m^2}{2m}$. So the sum in question is less than

$$\sum_{m=1}^{n-1} \sum_{k=m^2+1}^{m^2+2m} \frac{k-m^2}{2m} = \sum_{m=1}^{n-1} \sum_{\ell=1}^{2m} \frac{\ell}{2m} = \sum_{m=1}^{n-1} \left(m + \frac{1}{2}\right) = \frac{n^2-1}{2}. \qquad \square$$

**Example 3.32.** (2002 Belarusian Mathematical Olympiad) Let $\alpha_1$, …, $\alpha_n$ be rational numbers satisfying

$$\sum_{i=1}^{n} \{k\alpha_i\} < \frac{n}{2}$$

for every positive integer $k$.

(i) Prove that at least one of $\alpha_1, \ldots, \alpha_n$ is an integer.

(ii) Do there exist $\alpha_1, \ldots, \alpha_n$ that satisfy, for every integer $k \ge 1$,

$$\sum_{i=1}^{n} \{k\alpha_i\} \le \frac{n}{2},$$

such that no $\alpha_i$ is an integer?

**Solution.** Suppose for a contradiction that $\alpha_1, \dots, \alpha_n$ are not integers. We observe that $\{k\alpha\} = \{k\lfloor\alpha\rfloor + k\{\alpha\}\} = \{k\{\alpha\}\}$. So by replacing $\alpha_i$ by $\{\alpha_i\}$, we can assume that $0 < \alpha_i < 1$ and write $\alpha_i = a_i/b_i$ where $1 \le a_i < b_i$. Let $M = \prod_{i=1}^{n} b_i$. Then $(M-1)\alpha_i + \alpha_i = M\alpha_i \in \mathbb{Z}$, which implies that $\{(M-1)\alpha_i\} + \{\alpha_i\} = 1$. Summing $i = 1, 2, \dots, n$, we obtain

$$n = \sum_{i=1}^{n} 1 = \sum_{i=1}^{n} \{(M-1)\alpha_i\} + \sum_{i=1}^{n} \{\alpha_i\} < n,$$

which is a contradiction. For (ii), we can take $\alpha_i = \frac{1}{2}$ for all $i$. ☐

Before ending this section, we record another result that looks symmetric as shown below.

**Example 3.33.** (Guersenzvaig and Spivey [**163**]) Let $n, k \in \mathbb{N}$. Show that

$$\sum_{d=1}^{k} \lfloor n/d \rfloor - \sum_{d=\lfloor n/k \rfloor + 1}^{n} \lfloor n/d \rfloor = k \left\lfloor \frac{n}{k} \right\rfloor. \tag{3.21}$$

In addition, if $j \le k \le n$, prove that

$$\sum_{d=j+1}^{k} \lfloor n/d \rfloor - \sum_{d=\lfloor n/k \rfloor + 1}^{\lfloor n/j \rfloor} \lfloor n/d \rfloor = k \lfloor n/k \rfloor - j \lfloor n/j \rfloor. \tag{3.22}$$

**Solution.** If $k > n$, then both sides are zero and we are done. So assume that $k \le n$. Applying Theorem 3.20 to the function

$$f : [1, k] \to \left[\frac{n}{k}, n\right] \text{ given by } f(x) = \frac{n}{x},$$

we obtain

$$\sum_{1 \le d \le k} \lfloor n/d \rfloor - \sum_{\frac{n}{k} \le d \le n} \lfloor n/d \rfloor = k \left\lceil \frac{n}{k} - 1 \right\rceil. \tag{3.23}$$

If $k \mid n$, then (3.23) becomes

$$\sum_{1 \le d \le k} \lfloor n/d \rfloor - \sum_{d=\frac{n}{k}+1}^{n} \lfloor n/d \rfloor - \lfloor n/(n/k) \rfloor = k\left(\frac{n}{k} - 1\right),$$

which leads to (3.21). Suppose $k \nmid n$. Then the left-hand side of (3.23) and (3.21) are the same. In addition, $\left\lceil \frac{n}{k} - 1 \right\rceil = \left\lfloor \frac{n}{k} \right\rfloor$, so (3.21) is proved.

For the second part, we can write the left-hand side of (3.22) as

$$\left(\sum_{d=1}^{k} \lfloor n/d\rfloor - \sum_{d=1}^{j} \lfloor n/d\rfloor\right) - \left(\sum_{d=\lfloor n/k\rfloor+1}^{n} \lfloor n/d\rfloor - \sum_{d=\lfloor n/j\rfloor+1}^{n} \lfloor n/d\rfloor\right)$$
$$= \left(\sum_{d=1}^{k} \lfloor n/d\rfloor - \sum_{d=\lfloor n/k\rfloor+1}^{n} \lfloor n/d\rfloor\right) - \left(\sum_{d=1}^{j} \lfloor n/d\rfloor - \sum_{d=\lfloor n/j\rfloor+1}^{n} \lfloor n/d\rfloor\right)$$

and apply the first part to obtain the right-hand side of (3.22). □

## 3.5. Exercises

3.5.1 Draw the graph of the floor function, the ceiling function, and the function mapping $x$ to the fractional part of $x$.

3.5.2 Find all possible values of the following expressions when $x$ and $y$ run over all real numbers.

$$\lfloor x\rfloor - \lceil x\rceil, \lfloor -x\rfloor + \lceil x\rceil, \lfloor x\rfloor + \lceil -x\rceil, \lfloor -x\rfloor + \lceil -x\rceil,$$
$$\lfloor x\rfloor + \lceil x\rceil, \lfloor -x\rfloor - \lceil x\rceil, \lfloor x\rfloor - \lceil -x\rceil, \lfloor -x\rfloor - \lceil -x\rceil,$$
$$\lceil x+y\rceil - \lceil x\rceil - \lceil y\rceil, \text{ and } \{x+y\} - \{x\} - \{y\}.$$

3.5.3 Let $x, y \in \mathbb{R}$. Prove that $\lfloor 2x\rfloor - 2\lfloor x\rfloor$ is either 0 or 1. Show also that
(i) $\lfloor 2x\rfloor + \lfloor 2y\rfloor \ge \lfloor x\rfloor + \lfloor y\rfloor + \lfloor x+y\rfloor$,
(ii) $\lfloor 3x\rfloor + \lfloor 3y\rfloor \ge \lfloor x\rfloor + \lfloor y\rfloor + 2\lfloor x+y\rfloor$, and
(iii) $\lfloor 4x\rfloor + \lfloor 4y\rfloor \ge \lfloor x\rfloor + \lfloor y\rfloor + 3\lfloor x+y\rfloor$.

3.5.4 Let $d$, $n$, $m$ be positive integers. Show that
(i) $d \le \lfloor n/m\rfloor$ if and only if $m \le \lfloor n/d\rfloor$,
(ii) $\lfloor n/m\rfloor = d$ if and only if $\lfloor n/d+1\rfloor < m \le \lfloor n/d\rfloor$,
(iii) $d \le \lfloor n/\lfloor n/d\rfloor\rfloor$,
(iv) $\lfloor n/\lfloor n/\lfloor n/d\rfloor\rfloor\rfloor = \lfloor n/d\rfloor$.

3.5.5 Let $x \in \mathbb{R}$, $m \in \mathbb{Z}$, and $n \in \mathbb{N}$. Show that
(i) $\left\lfloor \frac{m+\lfloor -x\rfloor}{n}\right\rfloor = \left\lfloor \frac{m-x}{n}\right\rfloor$,
(ii) $\left\lceil \frac{m+\lceil -x\rceil}{n}\right\rceil = \left\lceil \frac{m-x}{n}\right\rceil$,
(iii) $\left\lceil \frac{m+\lfloor -x\rfloor}{n}\right\rceil = \left\lceil \frac{m-x-[x\notin\mathbb{Z}]}{n}\right\rceil$,
(iv) $\left\lfloor \frac{m+\lceil -x\rceil}{n}\right\rfloor = \left\lfloor \frac{m-x+[x\in\mathbb{Z}]}{n}\right\rfloor$.
Here we use the Iverson notation; for instance, in the statement (iv), the notation $[x \in \mathbb{Z}]$ is 1 if $x \in \mathbb{Z}$ and 0 otherwise.

Use some of these to give another solution to the problem given in Example 3.8.

3.5.6 Find all $x \in \mathbb{R}$ such that $\lceil \lfloor x \rfloor \rceil = \lfloor \lceil x \rceil \rfloor$.

3.5.7 Determine all nonnegative real numbers $x$ satisfying each of the following conditions.

(i) $\left\lfloor \sqrt{x} \right\rfloor = \sqrt{\lfloor x \rfloor}$,
(ii) $\left\lceil \sqrt{x} \right\rceil = \sqrt{\lceil x \rceil}$,
(iii) $\left\lceil \sqrt{x} \right\rceil = \sqrt{\lfloor x \rfloor}$,
(iv) $\left\lfloor \sqrt{x} \right\rfloor = \sqrt{\lceil x \rceil}$,
(v) $\left\lceil \sqrt{x} \right\rceil = \left\lfloor \sqrt{x} \right\rfloor$,
(vi) $\sqrt{\lfloor x \rfloor} = \sqrt{\lceil x \rceil}$
(vii) $\left\lceil \sqrt{\lfloor x \rfloor} \right\rceil = \left\lceil \sqrt{x} \right\rceil$,
(viii) $\left\lfloor \sqrt{\lceil x \rceil} \right\rfloor = \left\lfloor \sqrt{x} \right\rfloor$.

3.5.8 Let $m \in \mathbb{Z}$. Show that

$$A(m) = \left\lfloor \frac{3m+4}{13} \right\rfloor - \left\lfloor \frac{m - 28 - \left\lfloor \frac{m-7}{13} \right\rfloor}{4} \right\rfloor$$

is independent of $m$.

3.5.9 Solve the following equations.

(i) $\lfloor x \rfloor^2 - 2\lfloor x \rfloor - 3 = 0$,
(ii) $\lceil x \rceil^2 - 2\lfloor x \rfloor - 3 = 0$,
(iii) $\lfloor x \rfloor^2 - 2\lceil x \rceil - 3 = 0$,
(iv) $\lceil x \rceil^2 - 2\lceil x \rceil - 3 = 0$.
(v) $\left\lfloor x^2 \right\rfloor - 2\lfloor x \rfloor - 3 = 0$,
(vi) $\left\lceil x^2 \right\rceil - 2\lfloor x \rfloor - 3 = 0$,
(vii) $\left\lfloor x^2 \right\rfloor - 2\lceil x \rceil - 3 = 0$,
(viii) $\left\lceil x^2 \right\rceil - 2\lceil x \rceil - 3 = 0$.

3.5.10 Let $f(x) = x - \lfloor x \rfloor - \frac{1}{2}$ for every $x \in \mathbb{R}$. Show that

$$\left| \sum_{n=1}^{m} f\left(2^n x + \frac{1}{2}\right) \right| \leq 1 \quad \text{for all } m \geq 1 \text{ and all } x \in \mathbb{R}.$$

3.5.11 Let $m$ be a positive integer. Show that

$$\sum_{k=0}^{m} \left( \left\lfloor \frac{3^k + m}{3^{k+1}} \right\rfloor - \left\lfloor \frac{3^k - m}{3^{k+1}} \right\rfloor \right) = \begin{cases} m-1, & \text{if } \frac{m}{3^{v_3(m)}} \equiv 1 \pmod{3}; \\ m, & \text{if } \frac{m}{3^{v_3(m)}} \equiv 2 \pmod{3}. \end{cases}$$

3.5.12 Let $m, n \in \mathbb{N}$ be odd and $\gcd(m,n) = 1$. Let $a = (n-1)/2$, $b = (m-1)/2$.

(i) Prove that $\sum_{r=1}^{a} \lfloor mr/n \rfloor + \sum_{r=1}^{b} \lfloor nr/m \rfloor = ab$.

(ii) Obtain a corresponding result if $(m,n) = d$.

3.5.13 Prove that for each positive integer $n$,

$$\left\lfloor \sqrt{n} + \sqrt{n+1} \right\rfloor = \left\lfloor \sqrt{4n+1} \right\rfloor = \left\lfloor \sqrt{4n+2} \right\rfloor = \left\lfloor \sqrt{4n+3} \right\rfloor.$$

3.5.14 Let $r \in \mathbb{N}$ and $r \geq 2$. Determine the positive integers $n$ such that $\left\lfloor \sqrt[r]{n} \right\rfloor$ divides $n$.

3.5.15 Prove that

$$\sum_{k=1}^{n} \left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor \frac{n^2}{4} \right\rfloor$$

and that

$$\sum_{k=1}^{n} \left\lfloor \frac{k}{3} \right\rfloor = \left\lfloor \frac{n(n-1)}{6} \right\rfloor.$$

3.5.16 Prove that for each $a = 1, 2, \ldots, 7$, there exists an integer $b$ (depending on $a$) such that

$$\sum_{k=1}^{n} \left\lfloor \frac{k}{a} \right\rfloor = \left\lfloor \frac{(2n+b)^2}{8a} \right\rfloor.$$

3.5.17 Let $a, n \in \mathbb{N}$ and $(a, n) = 1$. Show that

$$\sum_{k=0}^{n-1} \left\lfloor x + \frac{ka}{n} \right\rfloor = \frac{(a-1)(n-1)}{2} + \lfloor nx \rfloor.$$

3.5.18 (1981 USA Mathematical Olympiad) Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Show that

$$\lfloor nx \rfloor \geq \frac{\lfloor x \rfloor}{1} + \frac{\lfloor 2x \rfloor}{2} + \frac{\lfloor 3x \rfloor}{3} + \cdots + \frac{\lfloor nx \rfloor}{n}.$$

3.5.19 Let $p$ be a prime and $n \in \mathbb{N}$. Show that

$$\frac{n}{p-1} - \left\lfloor \frac{\log n}{\log p} \right\rfloor - 1 \leq v_p(n!) \leq \frac{n-1}{p-1}.$$

Prove also that $\frac{n}{p} - 1 < v_p(n!) < \frac{n}{p} + \frac{n}{p(p-1)}$.

3.5.20 Let $f(n) = \left\lfloor \sqrt{n} \right\rfloor - \left\lfloor \sqrt{n-1} \right\rfloor$. Prove that $f$ is multiplicative but not completely multiplicative.

3.5.21 This exercise is to give another proof of Theorem 3.10. Prove the following.

(i) Let $x \in \mathbb{R}$, $m \in \mathbb{N}$, and $0 \le a_0 < a_1 < \cdots < a_{m-1} < 1$. Show that

$$\sum_{k=0}^{m-1} \lfloor x + a_k \rfloor = m \lfloor x \rfloor + m - r_m(x),$$

where $r_m(x)$ is equal to $\min(\{m\} \cup \{k \mid 0 \le k \le m-1 \text{ and } a_k \ge 1 - \{x\}\})$ which is also equal to $\min\{k \mid a_k \ge 1 - \{x\}\}$ if $a_{m-1} \ge 1 - \{x\}$ and $m$ otherwise. We remark that the set

$$\{k \mid a_k \ge 1 - \{x\}\}$$

may be empty and then $r_m(x)$ will be equal to $m$.

(ii) Give another proof of Theorem 3.10 by using (i). Let $x \in \mathbb{R}$, $m, n \in \mathbb{Z}$, and $0 \le m \le n$. Prove that

$$\sum_{0 \le k \le m-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \max\{m \lfloor x \rfloor, m \lfloor x \rfloor + m - n + \lfloor n\{x\} \rfloor\}.$$

3.5.22 Give another proof of Mortici's result [**276**] by applying Exercise 3.5.21.

(i) Let $m, n \in \mathbb{N}$ and $0 \le a_0 < a_1 < \cdots < a_{n-1} < 1$. Suppose that

$$\sum_{k=0}^{n-1} \lfloor x + a_k \rfloor = \lfloor mx \rfloor \quad \text{holds for all } x \in \mathbb{R}.$$

Show that $m = n$ and $a_k = \frac{k}{n}$ for every $k$.

(ii) Let $m, n \in \mathbb{N}$ and let $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_m$ be real numbers. Suppose

$$\sum_{k=1}^{n} \lfloor x + a_k \rfloor = \sum_{k=1}^{m} \lfloor x + b_k \rfloor \quad \text{holds}$$

for infinitely many integers $x \ge 1$. Show that $n = m$.

## 3.6. Notes

The presentation of Theorem 3.10 to Theorem 3.13 and Exercise 3.5.17 are taken from Aursukaree et al. [**20**]. Example 3.14 and many others are collected from various sources including problems from mathematical competitions but we also add something different such as those given in Example 3.7 and Exercises 3.5.5, 3.5.7, 3.5.9, and 3.5.11. In fact, the author used some parts of this chapter in the training for the International Mathematical Olympiad (IMO) for the students at the Institute for the Promotion of Teaching Science and Technology (IPST), Thailand. Theorem 3.17 is new and appears for the first time in this book. The counting argument as given in Theorems 3.18 to 3.21 has been known since the time of Gauss and Eisenstein (see for example in [**109**,**141**,**241**,**242**,**375**]). But, as far as we are aware, these theorems are new and the collection of them has not been given in the literature before.

As mentioned in the introduction, the Iverson notations $\lfloor x\rfloor$, $\lceil x\rceil$, and $[P]$ are convenient tools for certain types of calculations in number theory and combinatorics. The reader can see some examples in Graham, Knuth and Patashnik [**152**], Phunphayap and Pongsriiam [**294**], Pongsriiam and Subwattanachai [**325**], and Kawsumarng et al. [**218**]. For instance, in determining the $p$-adic valuation of Fibonomial coefficients, Phunphayap and Pongsriiam [**294**, Theorem 7] show that if $a \geq 0$, $\ell \geq 0$, $m \geq 1$ are integers, $p$ is a prime, and $p \equiv \pm 1 \pmod{m}$, then the $p$-adic valuation of the factorial $\left\lfloor \frac{\ell p^a}{m} \right\rfloor!$ is equal to

$$\frac{\ell(p^a-1)}{m(p-1)} - a\left\{\frac{\ell}{m}\right\} + \nu_p\left(\left\lfloor\frac{\ell}{m}\right\rfloor!\right), \text{ if } p \equiv 1 (\mathrm{mod} m);$$

$$\frac{\ell(p^a-1)}{m(p-1)} - \frac{a}{2}\delta + \nu_p\left(\left\lfloor\frac{\ell}{m}\right\rfloor!\right), \text{ if } p \equiv -1 (\mathrm{mod} m) \text{ and } a \text{ is even};$$

$$\frac{\ell(p^a-1)}{m(p-1)} - \frac{a-1}{2}\delta - \left\{\frac{\ell}{m}\right\} + \nu_p\left(\left\lfloor\frac{\ell}{m}\right\rfloor!\right), \text{ if } p \equiv -1 (\mathrm{mod} m)$$

and $a$ is odd,

where $\delta = [\ell \not\equiv 0 \pmod{m}]$ is the Iversion bracket.

Some problems in the exercises and their generalizations can be assigned as a homework or a short project for undergraduate students. For example, questions related to Exercise 3.5.3 are the following. If $n \geq 5$ is given, is it true that $\lfloor nx\rfloor + \lfloor ny\rfloor \geq \lfloor x\rfloor + \lfloor y\rfloor + (n-1)\lfloor x+y\rfloor$? If not, how can this be adjusted so that the corresponding inequality holds? What is a sharp lower bound for $\lfloor nx\rfloor + \lfloor ny\rfloor + \lfloor nz\rfloor$ in terms of $\lfloor x\rfloor$, $\lfloor y\rfloor$, $\lfloor z\rfloor$, $\lfloor x+y\rfloor$, $\lfloor x+z\rfloor$, and $\lfloor y+z\rfloor$? In general, can we generalize the result for the sum $\lfloor nx_1\rfloor + \lfloor nx_2\rfloor + \cdots + \lfloor nx_m\rfloor$? The solution to Example 3.30 implies that the number of positive integers $n \leq x$ such that $\left\lfloor\sqrt{n}\right\rfloor$ divides

$n$ is $3\sqrt{x}+O(1)$. Suppose $r \geq 3$ is given. Can we find a good approximation for the number of positive integers $n \leq x$ such that $\left\lfloor \sqrt[r]{n} \right\rfloor$ divides $n$? We know from Exercise 3.5.16 that for each $a \in \{1, 2, \dots, 7\}$, there exists $b \in \mathbb{Z}$, depending on $a$, such that $\sum_{k=1}^{n} \lfloor k/a \rfloor$ is equal to $\left\lfloor (2n+b)^2/8a \right\rfloor$. Pongsriiam and his coauthors [**292**] also showed that the choice of $b$ is unique for each $a = 1, 2, \dots, 7$ and that a simple formula like this does not exist for any $a \geq 8$.

Richman [**343**] extended Exercise 3.5.18 and determined the set of values $\lfloor nx \rfloor - \sum_{1 \leq m \leq n} \lfloor mx \rfloor / m$ as $n$ and $x$ vary. The sums similar to Exercise 3.5.13 were also investigated by some mathematicians. For example, the following holds for all $n \in \mathbb{N}$.

$$\lfloor \sqrt{n} + \sqrt{n+1} + \sqrt{n+2} \rfloor = \lfloor \sqrt{9n+8} \rfloor, \tag{3.24}$$

$$\lfloor \sqrt{n} + \sqrt{n+1} + \sqrt{n+2} + \sqrt{n+3} \rfloor = \lfloor \sqrt{16n+20} \rfloor, \tag{3.25}$$

$$\lfloor \sqrt{n} + \sqrt{n+1} + \sqrt{n+2} + \sqrt{n+3} + \sqrt{n+4} \rfloor = \lfloor \sqrt{25n+49} \rfloor. \tag{3.26}$$

The formula (3.24) was proposed by Hammer [**169**] as a problem in the *American Mathematical Monthly*; (3.25) was published by Wang [**433**]; and (3.26) was proved by Zhan [**441**]. The most general results in this direction were obtained by Saltzman and Yuan [**353**]. Among other things, Saltzman and Yuan [**353**, Theorem 2.3] extended the above formulas to

$$\left\lfloor \sum_{\ell=0}^{k-1} \sqrt[r]{n+\ell} \right\rfloor = \left\lfloor \sqrt[r]{k^r n + \frac{k^r(k-1)}{2} - 1} \right\rfloor,$$

which holds for $n > \frac{k^r(k-1)(2k-1)(r-1)}{12r}$ and $r, k \geq 2$. Then Kuhapatanakul and Ruankong [**234**] improved Lemma 2.2 of [**353**] and obtained the formula

$$\left\lfloor \sum_{\ell=0}^{k-1} \sqrt{n+\ell q} \right\rfloor = \left\lfloor \sqrt{k^2 n + \frac{qk^2(k-1)}{2} - 1} \right\rfloor,$$

for $q \in \mathbb{Q}$, $k \geq 2$, $n \geq \frac{q^2k^2(k^2-1)-12q}{24}$ with $qk \in \mathbb{Z}$. They [**350**] also gave another proof of Theorem 2.3 of Saltzman and Yuan [**353**] with a larger range of $n$. In general, if $r \geq 2$ and $a_1, a_2, \dots, a_k$ is a sequence with some nice properties, can we find a formula for

$$\left\lfloor \sqrt[r]{n+a_1} + \sqrt[r]{n+a_2} + \cdots + \sqrt[r]{n+a_k} \right\rfloor?$$

Other sums which involve the floor function have also been studied. Jacobsthal [**215**] introduced the sum $S_{a,b;m}(K)$, which was later generalized by Tverberg [**416**] to the following form: let $m$ and $\ell$ be positive integers and let $C$ be a multiset of $\ell$ integers $a_1, a_2, \dots, a_\ell$, i.e., $a_i = a_j$ is allowed for some $i \neq j$. Define $f_{C;m} : \mathbb{Z} \to \mathbb{Z}$ and $S_{C;m} : \mathbb{N} \cup \{0\} \to \mathbb{Z}$ by

$$\begin{aligned} f_{C;m}(k) &= \sum_{T \subseteq [1,\ell]} (-1)^{\ell-|T|} \left\lfloor \frac{k + \sum_{i \in T} a_i}{m} \right\rfloor, \\ S_{C;m}(K) &= \sum_{k=0}^{K} f_{C;m}(k). \end{aligned}$$

We sometimes write $f_{a_1,a_2,\dots,a_\ell;m}(k)$ and $S_{a_1,a_2,\dots,a_\ell;m}(K)$ instead of $f_{C;m}(k)$ and $S_{C;m}(K)$, respectively. The set $[1, \ell]$ appearing in the sum defining $f$ is the set of integers $1, 2, 3, \dots, \ell$. If $T = \emptyset$, then $\sum_{i \in T} a_i$ is defined to be zero. For example, if $C = \{a_1, a_2, a_3\}$, then $f_{C;m}(k)$ is given by

$$\begin{aligned} f_{a_1,a_2,a_3;m}(k) = &\left\lfloor \frac{a_1 + a_2 + a_3 + k}{m} \right\rfloor - \left\lfloor \frac{a_1 + a_2 + k}{m} \right\rfloor \\ &- \left\lfloor \frac{a_1 + a_3 + k}{m} \right\rfloor - \left\lfloor \frac{a_2 + a_3 + k}{m} \right\rfloor + \left\lfloor \frac{a_1 + k}{m} \right\rfloor \\ &+ \left\lfloor \frac{a_2 + k}{m} \right\rfloor + \left\lfloor \frac{a_3 + k}{m} \right\rfloor - \left\lfloor \frac{k}{m} \right\rfloor. \end{aligned}$$

Jacobsthal [**215**] showed that for any $K \in \mathbb{N} \cup \{0\}$, we have

$$0 \le S_{a,b;m}(K) \le \left\lfloor \frac{m}{2} \right\rfloor. \tag{3.27}$$

Carlitz [**73, 74**] and Grimson [**161**] gave an alternative proof of (3.27). Then using only elementary arguments, Tverberg [**416**] showed that (3.27) holds and stated without proof that $S_{a_1,a_2,a_3;m}(K) \le \lfloor m/3 \rfloor$ which was later verified by Thanatipanonda and Wong [**409**].

Onphaeng and Pongsriiam [**291**] obtained sharp lower and upper bounds of $f_{a_1,a_2,\dots,a_\ell;m}(k)$ for all $\ell \geq 2$. They also obtained a bound for $S_{a_1,a_2,\dots,a_\ell;m}(K)$, which is a sharp lower bound when $\ell$ is odd and a sharp upper bound when $\ell$ is even. More precisely, they obtained the following results.

**Theorem 3.34.** (Onphaeng and Pongsriiam [**291**, Theorem 8]) *For each* $\ell \geq 2$, $a_1, a_2, \dots, a_\ell, k \in \mathbb{Z}$ *and* $m \geq 1$, *we have*

$$-2^{\ell-2} \leq f_{a_1,a_2,\dots,a_\ell;m}(k) \leq 2^{\ell-2}.$$

*Moreover,* $-2^{\ell-2}$ *and* $2^{\ell-2}$ *are best possible in the sense that there are* $a_1, a_2, \dots, a_\ell$, $m$, $k$ *which makes the inequality become an equality.*

**Theorem 3.35.** (Onphaeng and Pongsriiam [**291**, Theorem 9]) *For each* $\ell \geq 2$, $a_1, a_2, \dots, , a_\ell \in \mathbb{Z}$, $m \in \mathbb{N}$, *and* $K \in \mathbb{N} \cup \{0\}$, *we have*

$$-2^{\ell-2} \left\lfloor \frac{m}{2} \right\rfloor \leq S_{a_1,a_2,\dots,a_\ell;m}(K) \leq 2^{\ell-2} \left\lfloor \frac{m}{2} \right\rfloor. \tag{3.28}$$

*Moreover, If* $\ell$ *is odd, then the lower bound* $-2^{\ell-2} \left\lfloor \frac{m}{2} \right\rfloor$ *is sharp and if* $\ell$ *is even, then the upper bound* $2^{\ell-2} \left\lfloor \frac{m}{2} \right\rfloor$ *is sharp in the sense that there are* $a_1, a_2, \dots, a_\ell$, $m$, $k$ *which makes the inequality become an equality.*

Hence half of the problem in determining sharp bounds for

$$S_{a_1,a_2,\dots,a_\ell;m}(K)$$

is solved. Thanatipanonda and Wong [**409**] predicted the bounds for some of the remaining cases. For more details, we refer the reader to [**291**] and [**409**]. To summarize, the following questions are open and we leave them to the interested reader.

> What is a sharp upper bound for $S_{a_1,a_2,\dots,a_\ell;m}(K)$ when $\ell$ is odd?
>
> What is a sharp lower bound for $S_{a_1,a_2,\dots,a_\ell;m}(K)$ when $\ell$ is even?

One of the most studied sequences related to the floor function are the Beatty sequences. For $x, x_0 \in \mathbb{R}$, the *homogeneous Beatty sequence* $B(x)$ and *inhomogeneous Beatty sequence* $B(x, x_0)$ are defined by

$$B(x) = (\lfloor nx \rfloor)_{n\geq 1} \quad \text{and} \quad B(x, x_0) = (\lfloor nx + x_0 \rfloor)_{n\geq 1}.$$

Depending on the context, it is sometimes more convenient to consider them as sets $\{\lfloor nx \rfloor \mid n \geq 1\}$ and $\{\lfloor nx + x_0 \rfloor \mid n \geq 1\}$, respectively. The starting point $n \geq 1$ may be replaced by $n \geq 0$, or $n \geq N$ for any $N \in \mathbb{Z}$, or $n$ may range over all integers, but for our discussion, it is always $n \geq 1$. It is well known that if $x$ and $y$ are positive irrational numbers satisfying $1/x + 1/y = 1$, then $B(x)$ and $B(y)$ form a partition of $\mathbb{N}$, that is,

$$B(x) \cup B(y) = \mathbb{N} \text{ and } B(x) \cap B(y) = \emptyset.$$

This result was proposed by Beatty [**40**, **41**] in 1926 as a problem in the *American Mathematical Monthly*, and before that, a special case of Beatty sequences called Wythoff sequences had already appeared as a solution to certain combinatorial games [**439**]. Since Wythoff sequences arise very often in combinatorics and combinatorial game theory, and so many of their combinatorial properties have been extensively studied; see for example in the work of Fraenkel [**126**, **129–131**], Kimberling [**223**, **224**], Pitman [**298**], Wythoff [**439**], and in the online encyclopedia OEIS [**374**].

Number theorists are also interested in Beatty sequences because they can be considered as a generalization of arithmetic progressions. In fact, if $x$ and $x_0$ are integers, then $B(x, x_0)$ is an arithmetic progression with the common difference $x$. For results on generalizations of Beatty's theorem and Beatty sequences, see for example, in the articles by Uspensky [**417**], Fraenkel [**126–128**], Graham [**151**], Tijdeman [**410**], Barat and Varju [**34**, **35**], Tadee and Laohakosol [**394**], Simpson [**372**], Technau [**406**], and Hildebrand, X. Li, J. Li, and Xie [**185**].

In particular, Fraenkel [**127**] observed that for each $m \geq 2$, if

$$\alpha_i = (2^m - 1)/2^{i-1} \quad \text{and} \quad \beta_i = -2^{m-i} + 1 \quad \text{for } 1 \leq i \leq m, \tag{3.29}$$

then $\{B(\alpha_i, \beta_i) \mid 1 \leq i \leq m\}$ forms a partition of $\mathbb{N}$. There is no significantly different example, and so Fraenkel made the following conjecture.

**Conjecture 3.36.** (Fraenkel [**127**]) Let $m \geq 3$ and $\alpha_1 > \alpha_2 > \cdots > \alpha_m$ be positive real numbers. If there are real numbers $\beta_1, \beta_2, \ldots, \beta_m$ such that $\{B(\alpha_i, \beta_i) \mid 1 \leq i \leq m\}$ forms a partition of $\mathbb{N}$, then (3.29) holds.

As far as we are aware, this is still open and the best result was obtained by Barat and Varju in [**34**], where they settled the conjecture for $m = 7$. For more details, we refer the reader to the references given above. For a recent result on some additive properties of Beatty sequences, see for instance, in the articles by Pongsriiam and his coauthors [**218**, **296**, **324**].

Chapter 4

# Summation Formulas

## 4.1. Introduction

The Riemann integral is defined as the limit of Riemann sums. In this sense, an integral can be approximated by a suitable sum and the readers might recall this from an exercise in calculus, real analysis, or numerical analysis courses. Conversely, a sum can also be estimated by a certain integral and we will do this in this chapter. Generally speaking, whenever we estimate $A$ by $B$, we should also know how close $A$ and $B$ are, or how large (or small) the errors $|A - B|$ or $|(A - B)/B|$ are. Therefore it is convenient to use a specific notation to indicate the size of the error occurring in the approximation or to compare the order of magnitude of functions. For example, both $(\log x)^3$ and $x^2$ tend to $\infty$ as $x \to \infty$ but $x^2$ grows more rapidly than $(\log x)^3$. More precisely, $\lim_{x\to\infty} \frac{(\log x)^3}{x^2} = 0$, which can be written by using the little $o$ notation as $(\log x)^3 = o(x^2)$. We will discuss this in more detail in the next section. Then we will give various basic summation formulas in subsequent sections. To prove such formulas conveniently, we also give a review on the Riemann-Stieltjes integral in Section 4.5. Finally, we remind the reader that $\log x$ is always the natural logarithm of $x$ (not the common logarithm of $x$) throughout this text.

## 4.2. Big $O$, Little $o$, and Related Notations

To compare the order of magnitude of functions, the notations such as $O$, $o$, $\sim$, $\ll$, and $\gg$ are used regularly in the literature and they are explained in this section. The notations $\ll$ and $\gg$ are introduced by Vinogradov and are popular among number theorists. Other symbols are also standard in number theory (see also the notes in Section 4.9). However, we should remark that they may be used in physics and other branches of mathematics or computer science with a different meaning. For example, one sometimes writes $f(x) \prec g(x)$ to mean that $f(x) = o(g(x))$ but we do not use $f(x) \prec g(x)$ in this text.

**4.2.1. Big $O$ and Vinogradov notations.** Let $a$ be a nonnegative real number, $f, g : [a, \infty) \to \mathbb{R}$, and $g(x) > 0$ for all $x \in [a, \infty)$. Then we write $f(x) = O(g(x))$ if there exists a constant $M > 0$ such that

$$|f(x)| \leq Mg(x) \quad \text{for all } x \in [a, \infty).$$

In particular, $f(x) = O(1)$ if $f$ is bounded on $[a, \infty)$. The order of magnitude of functions is sometimes considered in a neighborhood of a real number or of infinity. We write $f(x) = O(g(x))$ as $x \to \infty$ if there exist $a_0 \geq a$ and $M > 0$ such that $|f(x)| \leq Mg(x)$ for all $x \geq a_0$. If $c \in [a, \infty)$, then we write $f(x) = O(g(x))$ as $x \to c$ if there exist $\delta > 0$ and $M > 0$ such that

$$|f(x)| \leq Mg(x) \text{ for all } x \in (c - \delta, c + \delta) \cap [a, \infty).$$

In this text, when we use the big $O$ notation, we usually consider the functions in the whole domain. To make it clear, we sometimes write the statements such as

$$\begin{gathered}\text{“uniformly for } x \geq a,\ f(x) = O(g(x))\text{”or}\\ \text{“}f(x) = O(g(x)) \text{ for } x \geq a\text{”}\end{gathered}$$

to mean that there exists a constant $M > 0$ such that $|f(x)| \leq Mg(x)$ for all $x \geq a$. As usual, if we write $O(g(x))$ it is assumed that $g(x) > 0$ for all $x$ in the specified domain.

For Vinogradov's notation, $f(x) \ll g(x)$ is the same as $f(x) = O(g(x))$ and $f(x) \gg g(x)$ means $g(x) \ll f(x)$. Nevertheless, if we write $f(x) \gg g(x)$, then it is assumed that both $f(x)$ and $g(x)$ are positive for all $x$ in the domains.

The advantage of using Vinogradov's notation is that it is more convenient when we have a chain of estimates such as

$$f(x) \ll f_1(x) \ll f_2(x) \ll f_3(x) \text{ or } g(x) \gg f_4(x) \gg f_5(x).$$

As in a regular inequality, $f(x) \ll f_1(x) \ll f_2(x)$ means that

$$f(x) \ll f_1(x) \text{ and } f_1(x) \ll f_2(x).$$

On the other hand, if $f(x) - g(x) \ll h(x)$, it is often better to write $f(x) = g(x) + O(h(x))$. Finally, if $f(x) \ll g(x)$ and $g(x) \ll f(x)$, then we say that $f$ and $g$ *have the same order of magnitude* and write $f(x) \asymp g(x)$.

**4.2.2. Little $o$ notation and asymptotic relation $\sim$.** Again, let $f, g : [a, \infty) \to \mathbb{R}$, $a \geq 0$, and $g(x) > 0$ for all $x \in [a, \infty)$. We write $f(x) = o(g(x))$ as $x \to \infty$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. If $c \in [a, \infty)$ is a fixed real number, then we write $f(x) = o(g(x))$ as $x \to c$ if $\lim_{x\to c} \frac{f(x)}{g(x)} = 0$. Nevertheless, in this text, we do not consider the relation $f(x) = o(g(x))$ as $x$ approaches a point in $[a, \infty)$. So we simply write $f(x) = o(g(x))$ to mean $f(x) = o(g(x))$ as $x \to \infty$. In addition, we say that the functions $f$ and $g$ are *asymptotic* (or *asymptotically equivalent*) and we write

$$f(x) \sim g(x) \text{ if } \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

As in the case of big $O$, when we write $f(x) = o(g(x))$, it is automatically assumed that $g(x) > 0$ for all $x$ in the specified domain. For $f(x) \sim g(x)$, we only need $g(x) \neq 0$ for all large $x$ (but we still focus only on the case $g(x) > 0$). To help the readers get familiar with these symbols, we provide several examples as follows.

**Example 4.1.** Uniformly for $x \geq 1$, we have

(i) $3x^4 + 5x^3 + 10x + 1 = O(x^4)$,

(ii) $\frac{2}{x^2} + \frac{1}{x} + 1 = O(1)$,

(iii) $3x + (\log 5x)^4 \ll x$,

(iv) $e^x \cos x \ll e^x$.

**Solution.** For all $x \geq 1$, we have

$$|3x^4 + 5x^3 + 10x + 1| \leq 3x^4 + 5x^4 + 10x^4 + x^4 \leq 19x^4.$$

So (i) is proved. For (ii) and (iv), we have

$$|2/x^2 + 1/x + 1| \leq 2 + 1 + 1 = 4 \text{ and } |e^x \cos x| \leq e^x.$$

So it remains to prove (iii). Since $\lim_{x\to\infty}\frac{(\log 5x)^4}{x}=0$, there exists $x_0>1$ such that

$$\frac{(\log 5x)^4}{x}\le 1 \text{ for all } x\ge x_0.$$

Therefore

$$|3x+(\log 5x)^4|\le 3x+x=4x \text{ for all } x\ge x_0.$$

In addition, the function $x\mapsto \frac{3x+(\log 5x)^4}{x}$ is continuous on $[1,x_0]$, which is a compact set, so it has an upper bound, say $\alpha$, on $[1,x_0]$. If we let $M=\max\{4,\alpha\}$, then

$$3x+(\log 5x)^4\le Mx \text{ for all } x\ge 1.$$

Hence (iii) is verified. □

In general, suppose that $f$ and $g$ are continuous on $[1,\infty)$,

$$g(x)>0 \text{ for all } x\ge 1, \text{ and } \lim_{x\to\infty} f(x)/g(x)=0.$$

Then there exists $x_0>1$ such that $f(x)/g(x)\le 1$ for all $x\ge x_0$. Since $f/g$ is continuous, it is also bounded on the compact interval $[1,x_0]$, say

$$|f(x)/g(x)|\le\alpha \text{ for all } x\in[1,x_0].$$

So if $M=\{1,\alpha\}$, then $M$ is a constant that does not depend on $x$ and $|f(x)|\le Mg(x)$ for all $x\ge 1$. Therefore $f(x)=O(g(x))$ for $x\ge 1$. The argument of this type will be used throughout the text without further reference.

**Example 4.2.** Prove the following statements.

(i) As $x\to\infty$, $3x+(\log 5x)^4=o(x^2)$ but $3x+(\log 5x)^4$ is not $o(x)$. (This should be compared with (iii) in Example 4.1.)

(ii) As $x\to\infty$, $x=O(x^2)$ but $x^2$ is not $O(x)$.

(iii) For $x\ge 1$, $x=O(x^2)$ but $x^2$ is not $O(x)$.

(iv) As $x\to 0$, $x^2=O(x)$ but $x$ is not $O(x^2)$.

**Solution.** As $x\to\infty$, $\frac{3x+(\log 5x)^4}{x^2}$ converges to 0 and $\frac{3x+(\log 5x)^4}{x}$ converges to $3\ne 0$. So (i) is proved. Since $x\le x^2$ for all $x\ge 1$, we obtain $x=O(x^2)$ as $x\to\infty$. Suppose $x^2=O(x)$ as $x\to\infty$. Then there exist constants $a,M>0$ such that $x^2\le Mx$ for all $x\ge a$. Therefore $M\ge x$ for all $x\ge a$, which is a contradiction. This proves (ii). The proof of (iii) is similar to (ii), so we leave it to the reader. For the first part of (iv), we can choose $\delta = M = 1$ to see that $|x^2| \leq Mx$ for all $x \in (0, \delta)$. Finally, suppose that $x = O(x^2)$ as $x \to 0$. Then there are constants $\delta, M > 0$ such that $|x| \leq Mx^2$ for all $x \in (0, \delta)$. This implies that $1/x \leq M$ for all $x \in (0, \delta)$. But $1/x \to +\infty$ as $x \to 0^+$, so this is a contradiction. $\square$

Other examples are given below. The proof is left as an exercise to the reader.

**Example 4.3.** We have $\frac{1}{\log x} = o(1)$, $\sin x = o(\sqrt{x})$, $\sin x = o(\log x)$, $(\log x)^5 = o(x^{\frac{1}{3}})$, $x^4 = o(e^x)$. For $x \geq 1$, $\sin x = O(1)$, $(\log x)^3 = O(\sqrt{x})$, $x^{10} = O(e^x)$, and $x^2 = O(x^3)$. But it does not hold that $x^2 = O(x^3)$ for $x > 0$. For $x \geq 2$, we have $x \gg (\log x)^2$, $3x + 1 \gg 100x$, $x^2 \asymp 50x^2+6x+7$. As $x \to \infty$, we have $2x^2+5x+1 \sim 2x^2$, $2e^x+5x^{10}+1 \sim 2e^x$, $\frac{\sin(1/x)}{1/x} \sim 1$.

**Remark 4.4.** We have defined what it means to say that

$$f(x) = O(g(x)) \text{ but not } O(g(x)) \text{ in isolation.}$$

It is convenient to make our notations flexible. If we write $O(g(x))$, it means an unspecified function $f$ such that $f(x) = O(g(x))$. Then we can write, for example, $O(1) + O(1) = O(1)$ which means that if $f(x) = O(1)$ and $g(x) = O(1)$, then $f(x)+g(x) = O(1)$. The expression $\sum_{n=1}^{k} O(g(x))$ stands for the sum of unspecified functions $f_1, f_2, \ldots, f_k$ each of which is $O(g(x))$. In addition, if

$$f(x) - g(x) = O(h(x)) \text{ or } f(x) - g(x) = o(h(x)),$$

then we write

$$f(x) = g(x) + O(h(x)) \text{ and } f(x) = g(x) + o(h(x)),$$

respectively.

With the above convention, we have the following results.

**Theorem 4.5.** *Suppose that $a \geq 0$ and all functions are defined on the interval $[a, \infty)$. Then the following statements hold.*

(i) $O(g(x)) + O(g(x)) = O(g(x))$.

(ii) *If $f(x) = O(g(x))$ and $f(x) > 0$ for all $x$, then*

$$O(f(x)) + O(g(x)) = O(g(x)).$$

(iii) $\sum_{n=1}^{k} O(g_n(x)) = O\left(\sum_{n=1}^{k} g_n(x)\right)$.

(iv) $\int_1^t O(g(x))\ dx = O\left(\int_1^t g(x)\,dx\right)$ *(if the functions involved are integrable).*

(v) *If* $f(x) = g(x) + O(h(x))$, *then* $g(x) = f(x) + O(h(x))$.

*In addition, suppose that* $f/g$ *is bounded on every compact subset of* $[a, \infty)$. *Then we have*

(vi) *If* $f(x) = o(g(x))$, *then* $f(x) = O(g(x))$,

(vii) *If* $f(x) \sim g(x)$, *then* $f(x) = O(|g(x)|)$,

(viii) *If* $f(x) \sim g(x)$, *then* $f(x) = g(x) + o(|g(x)|)$.

**Proof.** For (i), let $f_1(x) = O(g(x))$ and $f_2(x) = O(g(x))$. Then there are $a_1, a_2 > a$ and $M_1, M_2 > 0$ such that $|f_1(x)| \le M_1 g(x)$ for all $x \ge a_1$ and $|f_2(x)| \le M_2 g(x)$ for all $x \ge a_2$. Let $a_3 = \max\{a_1, a_2\}$ and $M = M_1 + M_2$. Then

$$|f_1(x) + f_2(x)| \le |f_1(x)| + |f_2(x)| \le Mg(x) \quad \text{for all } x \ge a_3.$$

This proves (i). The proof of (ii), (iii), (iv), and (v) are similar to that of (i), so we leave it to the reader. Since (vi) and (vii) are also similar, we only prove (vii). Suppose that $\lim_{x\to\infty} f(x)/g(x) = 1$. Then there exists $x_0 > a$ such that $|f(x)/g(x) - 1| < 1$ for all $x > x_0$. Then

$$|f(x)| \le |f(x) - g(x)| + |g(x)| \le 2|g(x)|, \quad \text{for all } x > x_0.$$

This proves (vii). For (viii), suppose $\lim_{x\to\infty} f(x)/g(x) = 1$. Since $\frac{f(x)-g(x)}{|g(x)|}$ is equal to $f(x)/g(x) - 1$ or $-(f(x)/g(x) - 1)$ and they both converge to 0 as $x \to \infty$, we obtain $\frac{f(x)-g(x)}{|g(x)|} \to 0$ as $x \to \infty$. This completes the proof. □

## 4.3. Sums of Monotone Functions

Suppose that $I$ is an interval and $g : I \to \mathbb{R}$. Then $g$ is said to be *monotone* on $I$ if it is either increasing or decreasing on $I$. In addition, $g$ is said to be *unimodal* on $I$ if there exists $x_0 \in I$ such that $g$ is increasing on $I \cap (-\infty, x_0]$ and decreasing on $I \cap [x_0, \infty)$. Furthermore, if $g$ is monotone or unimodal on $[a, b]$, then $g$ is integrable on $[a, b]$. Let $f$ be an arithmetic function and define $F : [0, \infty) \to \mathbb{C}$ by $F(x) = \sum_{n\le x} f(n)$ where the sum is taken over all positive integers $n \le x$. Then, for instance, $F(x) = 0$ if $x < 1$, $F(x) = f(1)$ if $1 \le x < 2$, and $F(x) = f(1) + f(2)$ if $2 \le x < 3$.

In this section, we give an approximation for the sum $F(x)$ when $f$ is monotone or unimodal on $[1,x]$. Since the sum is empty when $x<1$, we usually assume that $x\geq 1$ or more generally $x\geq a$ for a large number $a$. So whenever the sum is empty or does not make sense for small values of $x$, it is assumed that $x$ is large.

**Theorem 4.6.** *The following statements hold.*

(i) *If $a$ and $b$ are integers with $a<b$ and $f$ is monotone on $[a,b]$, then*

$$\min\{f(a),f(b)\}\leq \sum_{n=a}^{b} f(n)-\int_a^b f(t)dt\leq \max\{f(a),f(b)\}.$$

(ii) *If $x,y\in\mathbb{R}$, $y<\lfloor x\rfloor$, and $f$ is nonnegative and monotone on $[y,x]$, then*

$$\left|\sum_{y<n\leq x} f(n)-\int_y^x f(t)dt\right|\leq \max\{f(y),f(x)\},\quad \textit{and}$$

$$\sum_{y<n\leq x} f(n)=\int_y^x f(t)dt+O\left(\max\{f(y),f(x)\}\right).$$

(iii) *If $f$ is nonnegative and unimodal on $[1,x]$, then*

$$\sum_{n\leq x} f(n)=\int_1^x f(t)dt+O(1).$$

**Proof.** Assume that $a,b\in\mathbb{Z}$, $a<b$, and $f$ is monotone on $[a,b]$. We first consider the case when $f$ is increasing. Then for $a\leq n\leq b-1$, we have

$$f(n)\leq \int_n^{n+1} f(t)dt\leq f(n+1).$$

Summing the above from $n=a$ to $n=b-1$, we obtain

$$\sum_{n=a}^{b-1} f(n)\leq \int_a^b f(t)\,dt\leq \sum_{n=a+1}^{b} f(n).$$

This implies that

$$f(a)\leq \sum_{n=a}^{b} f(n)-\int_a^b f(t)\,dt\leq f(b).$$

Similarly, if $f$ is decreasing on $[a,b]$, then

$$f(b) \le \sum_{n=a}^{b} f(n) - \int_a^b f(t)\,dt \le f(a).$$

This proves (i). Next let $x, y \in \mathbb{R}$, $y < \lfloor x \rfloor$, and let $f$ be nonnegative and monotone on $[y,x]$. Let $a = \lfloor y \rfloor + 1$ and $b = \lfloor x \rfloor$. Suppose that $f$ is increasing on $[y,x]$. By part (i), we obtain

$$\sum_{y<n\le x} f(n) = \sum_{n=a}^{b} f(n) \le f(b) + \int_a^b f(t)\,dt \le f(x) + \int_y^x f(t)\,dt, \tag{4.1}$$

$$\begin{aligned} \sum_{y<n\le x} f(n) &\ge f(a) + \int_a^b f(t)\,dt \\ &= f(a) + \int_y^x f(t)\,dt - \int_y^a f(t)\,dt - \int_b^x f(t)\,dt. \end{aligned} \tag{4.2}$$

Since $\int_y^a f(t)\,dt \le f(a)(a-y) \le f(a)$, (4.2) implies that

$$\sum_{y<n\le x} f(n) \ge \int_y^x f(t)\,dt - \int_b^x f(t)\,dt \ge \int_y^x f(t)\,dt - f(x). \tag{4.3}$$

From (4.1) and (4.3), we see that

$$\left| \sum_{y<n\le x} f(n) - \int_y^x f(t)\,dt \right| \le f(x) = \max\{f(y), f(x)\}.$$

Similarly, if $f$ is decreasing on $[y,x]$, then

$$\left| \sum_{y<n\le x} f(n) - \int_y^x f(t)\,dt \right| \le f(y) = \max\{f(y), f(x)\}.$$

This proves (ii). For (iii), let $f$ be increasing on $[1, x_0]$ and decreasing on $[x_0, x]$. Then we write

$$\sum_{n\le x} f(n) = f(1) + \sum_{1<n\le x_0} f(n) + \sum_{x_0<n\le x} f(n)$$

and apply part (ii) to obtain

$$\sum_{n\le x} f(n) = \int_1^{x_0} f(t)\,dt + \int_{x_0}^x f(t)\,dt + O(1) = \int_1^x f(t)\,dt + O(1).$$

This completes the proof. □

Next we give an example to show an application of Theorem 4.6. We remind the reader that when we consider the sum $\sum_{n\le x} f(n)$, we sometimes assume that $x$ is large so that the formula makes sense. For example, the equation (4.8) given below holds uniformly for $x \ge 2$, not for $x \ge 1$, since we would like $\log x$ to be positive and bounded away from zero. Nevertheless, the remaining formulas hold uniformly for $x \ge 1$.

**Example 4.7.** Let $\alpha \ge 0$ be a real number. Then the following hold.

$$\sum_{n\le x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O\left(x^\alpha\right). \tag{4.4}$$

$$\sum_{n\le x} \frac{1}{n^\alpha} = \frac{x^{-\alpha+1}}{-\alpha+1} + O(1) \quad (\text{for } \alpha > 0 \text{ and } \alpha \ne 1). \tag{4.5}$$

$$\sum_{n> x} \frac{1}{n^\alpha} = O\left(x^{-\alpha+1}\right) \quad (\text{for } \alpha > 1). \tag{4.6}$$

$$\sum_{n\le x} \frac{1}{n} = \log x + O(1). \tag{4.7}$$

$$\sum_{n\le x} \log n = x\log x - x + O(\log x). \tag{4.8}$$

$$\sum_{n\le x} n^\alpha \log n = \frac{x^{\alpha+1}}{\alpha+1}\left(\log x - \frac{1}{\alpha+1}\right) + O\left(x^\alpha \log x\right). \tag{4.9}$$

**Solution.** Let $\alpha \ge 0$. By Theorem 4.6, the left-hand side of (4.4) is

$$1 + \sum_{1<n\le x} n^\alpha = 1 + \int_1^x t^\alpha \, dt + O(x^\alpha) = 1 + \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O(x^\alpha).$$

Since $1 - \frac{1}{\alpha+1} \ll 1 \ll x^\alpha$, the above leads to (4.4). Next for $\alpha > 0$ and $\alpha \ne 1$, we have

$$\sum_{n\le x} \frac{1}{n^\alpha} = 1 + \int_1^x \frac{1}{t^\alpha}\, dt + O(1) = \frac{x^{-\alpha+1}}{-\alpha+1} + O(1).$$

Similarly, if $\alpha > 1$, then the left-hand side of (4.6) is

$$\lim_{y\to\infty}\left(\sum_{x<n\le y} \frac{1}{n^\alpha}\right) = \lim_{y\to\infty}\left(\frac{y^{-\alpha+1}}{-\alpha+1} - \frac{x^{-\alpha+1}}{-\alpha+1} + O\left(\frac{1}{x^\alpha}\right)\right),$$

which is $\frac{x^{-\alpha+1}}{-\alpha+1} + O(x^{-\alpha}) \ll x^{-\alpha+1}$. So (4.5) and (4.6) are proved. For (4.7) to (4.9), we have

$$\begin{aligned}
\sum_{n\le x} \frac{1}{n} &= 1 + \int_1^x \frac{1}{t}\, dt + O(1) = \log x + O(1),\\
\sum_{n\le x} \log n &= \sum_{1<n\le x} \log n = \int_1^x \log t\, dt + O(\log x)\\
&= x\log x - x + O(\log x),\\
\sum_{n\le x} n^\alpha \log n &= \sum_{1<n\le x} n^\alpha \log n = \int_1^x t^\alpha \log t dt + O(x^\alpha \log x).
\end{aligned}$$

Then (4.9) follows from the integration by part

$$\int t^\alpha \log t dt = \frac{t^{\alpha+1}}{\alpha+1}\log t - \int \frac{t^{\alpha+1}}{\alpha+1} = \frac{t^{\alpha+1}}{\alpha+1}\left(\log t - \frac{1}{\alpha+1}\right). \quad \square$$

## 4.4. Partial Summation Formula

Since Theorem 4.6 is applicable only to the sum $\sum_{n\le x} f(n)$ where $f$ is monotone or unimodal on $[1, x]$, we need a more flexible formula. In this section, we show a method of partial summations which can be applied to approximate the sum of the form $\sum_{n\le x} a_n f(n)$ when we have a good estimate for $\sum_{n\le x} a_n$.

**Theorem 4.8.** (Partial Summation: discrete version) *Let* $(a_n)_{n\ge1}$ *and* $(f(n))_{n\ge1}$ *be sequences of complex numbers and let* $1 \le c < b$ *be positive integers. For each* $N \in \mathbb{N}$*, let* $A(N) = \sum_{n=1}^{N} a_n$*. Then*

$$\sum_{n=c}^{b} a_n f(n) = A(b)f(b) - A(c-1)f(c) - \sum_{n=c}^{b-1} A(n)(f(n+1) - f(n)).$$

**Proof.** By a direct calculation and the change of variables, we obtain

$$\begin{aligned}\sum_{n=c}^{b} a_n f(n) &= \sum_{n=c}^{b} (A(n) - A(n-1)) f(n)\\
&= \sum_{n=c}^{b} A(n) f(n) - \sum_{n=c}^{b} A(n-1) f(n)\\
&= A(b)f(b) + \sum_{n=c}^{b-1} A(n) f(n) - \sum_{n=c}^{b} A(n-1) f(n)\\
&= A(b)f(b) + \sum_{n=c+1}^{b} A(n-1) f(n-1) - \sum_{n=c}^{b} A(n-1) f(n)\\
&= A(b)f(b) - A(c-1)f(c) + \sum_{n=c+1}^{b} A(n-1)(f(n-1) - f(n))\\
&= A(b)f(b) - A(c-1)f(c) - \sum_{n=c}^{b-1} A(n)(f(n+1) - f(n)).\end{aligned}$$ □

Theorem 4.8 leads to Abel's test for the convergence of series as shown in the next example.

**Example 4.9.** (Abel's Test) Suppose $\sum_{n=1}^{\infty} a_n$ is convergent and $(f(n))_{n\geq 1}$ is monotone convergent. Then $\sum_{n=1}^{\infty} a_n f(n)$ is convergent.

**Solution.** Let $1 < c < b$ be integers and let $A(N) = \sum_{n\leq N} a_n$. Then $A(N) \to A$ as $N \to \infty$, and $f(n) \to \ell$ as $n \to \infty$, for some $A, \ell \in \mathbb{R}$. By the partial summation formula,

$$\sum_{n=c}^{b} a_n f(n) = A(b)f(b) - A(c-1)f(c) - \sum_{n=c}^{b-1} A(n)(f(n+1) - f(n)).$$

As $c, b \to \infty$, $A(b)f(b) - A(c-1)f(c) \to 0$. In addition, if $N$ is large enough, then $|A(N) - A| < 1$. So if $c$ and $b$ are large enough, then

$$\begin{aligned}
&\left|\sum_{n=c}^{b-1} A(n)(f(n+1)-f(n))\right| \\
&\quad\le \sum_{n=c}^{b-1} |A(n)-A||f(n+1)-f(n)| + |A|\sum_{n=c}^{b-1} |f(n+1)-f(n)| \\
&\quad\le (1+|A|)\sum_{n=c}^{b-1} |f(n+1)-f(n)| = (1+|A|)|f(b)-f(c)|,
\end{aligned}$$

which converges to 0 as $b, c \to \infty$. By the Cauchy criterion, $\sum_{n=1}^{\infty} a_n f(n)$ converges. ☐

We will deal with the sum of the form $\sum_{y<n\le x} a_n f(n)$ where $x, y$ are real numbers (not necessarily integers) more often than that given in Theorem 4.8. Thus a different version of partial summation is more useful.

**Theorem 4.10.** (Abel's Summation Formula) *Suppose $(a_n)_{n\ge1}$ is a sequence of complex numbers and $f : [y,x] \to \mathbb{R}$ has a continuous derivative on the interval $[y,x]$, where $0 < y < x$. For each $x > 0$, let $A(x) = \sum_{n\le x} a_n$. Then*

$$\sum_{y<n\le x} a_n f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

**Proof.** We first consider the case $x \in \mathbb{Z}$ and show that

$$\sum_{n\le x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt. \tag{4.10}$$

Since the integral in (4.10) can be written as

$$\sum_{1\le m\le x-1} \int_m^{m+1} A(t)f'(t)dt$$

and $A(t) = A(m)$ for all $t$ in the interval $(m, m+1)$, we see that $\int_1^x A(t)f'(t)dt$ is equal to

$$\sum_{1\le m\le x-1} A(m)\int_m^{m+1} f'(t)dt = \sum_{1\le m\le x-1} A(m)(f(m+1)-f(m)).$$

Similar to the proof of Theorem 4.8, by distributing the sum and changing some variables, the above is equal to

$$-\sum_{2\le m\le x-1} a_m f(m) + A(x-1)f(x) - a_1 f(1).$$

So the right-hand side of (4.10) is

$$\begin{aligned} A(x)f(x) - A(x-1)f(x) + \sum_{2\le m\le x-1} a_m f(m) + a_1 f(1) \\ = \sum_{1\le m\le x} a_m f(m). \end{aligned}$$

This proves (4.10) when $x \in \mathbb{Z}$. Next assume that $x \notin \mathbb{Z}$. Then $\lfloor x \rfloor < x < \lfloor x \rfloor + 1$ and the left-hand side of (4.10) is

$$\begin{aligned} \sum_{n\le \lfloor x \rfloor} a_n f(n) &= A(\lfloor x \rfloor) f(\lfloor x \rfloor) - \int_1^{\lfloor x \rfloor} A(t) f'(t)dt \\ &= A(x) f(\lfloor x \rfloor) - \int_1^{x} A(t) f'(t)dt + \int_{\lfloor x \rfloor}^{x} A(t) f'(t)dt. \end{aligned}$$

Since $A(t) = A(x)$ for all $t \in (\lfloor x \rfloor, x)$, the last integral above is equal to $A(x)(f(x) - f(\lfloor x \rfloor))$, which leads to (4.10). Therefore (4.10) holds for any $x > 0$. Hence

$$\begin{aligned} &\sum_{y<n\le x} a_n f(n) = \sum_{n\le x} a_n f(n) - \sum_{n\le y} a_n f(n) \\ &= \left(A(x)f(x) - \int_1^x A(t)f'(t)dt\right) - \left(A(y)f(y) - \int_1^y A(t)f'(t)dt\right) \\ &= A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt, \text{ as desired.} \end{aligned}$$

□

Before showing some examples and applications of Theorem 4.10, we would like to give another proof of it. In fact, we can use the Riemann-Stieltjes integral to give a shorter and more natural proof of the Abel summation formula. It also leads to a more general result known as the Euler-Maclaurin summation formula. So we first give a review of this concept in the next section.

## 4.5. Review of the Riemann-Stieltjes Integral

Recall that the Riemann integral $\int_a^b f(x)\ dx$ is defined as the limit of Riemann sums $\sum_{i=1}^n f(t_i)\Delta x_i$. This can be generalized to the Riemann-Stieltjes integral $\int_a^b f(x)\ dg(x)$ as follows.

Let $P = \{x_0, x_1, \dots, x_n\}$ be a partition of $[a, b]$, where

$$a = x_0 < x_1 < x_2 < \cdots < x_n = b.$$

For each $i \in \{1, \dots, n\}$, let $x_{i-1} \le t_i \le x_i$. We form the sum

$$S(P, f, g) = \sum_{i=1}^{n} f(t_i)(g(x_i) - g(x_{i-1})).$$

We say that the Riemann-Stieltjes integral $\int_a^b f(x)\ dg(x)$ exists and is equal $\ell$ if for every $\varepsilon > 0$, there is a $\delta > 0$ such that $|S(P, f, g) - \ell| < \varepsilon$ whenever $x_i$ and $t_i$ are as above and $\|P\| = \max_{1\le i\le n} |x_i - x_{i-1}| \le \delta$. In this case, we say that $f$ is *Riemann integrable with respect to* $g$ on $[a, b]$ and write $f \in R(g)$. Some basic results concerning Riemann-Stieltjes integrals are as follows.

**Theorem 4.11.** *Assume that all functions are defined and bounded on* $[a, b]$. *Then the following statements hold.*

(i) *Let* $c_1$ *and* $c_2$ *be constants. If* $f_1 \in R(g)$ *and* $f_2 \in R(g)$ *on* $[a, b]$, *then* $c_1 f_1 + c_2 f_2 \in R(g)$ *on* $[a, b]$ *and*

$$\int_a^b (c_1 f_1(x) + c_2 f_2(x))\ dg(x) = c_1 \int_a^b f_1(x)\ dg(x) + c_2 \int_a^b f_2(x)\ dg(x).$$

*If* $f \in R(g_1)$ *and* $f \in R(g_2)$ *on* $[a, b]$, *then* $f \in R(c_1 g_1 + c_2 g_2)$ *on* $[a, b]$ *and*

$$\int_a^b f(x)\ d(c_1 g_1 + c_2 g_2)(x) = c_1 \int_a^b f(x)\ dg_1(x) + c_2 \int_a^b f(x)\ dg_2(x).$$

(ii) *If* $f$ *is continuous on* $[a, b]$ *and* $g$ *is of bounded variation on* $[a, b]$, *then the Riemann-Stieltjes integral* $\int_a^b f(x)\ dg(x)$ *exists.*

(iii) *If* $\int f(x)\ dg(x)$ *exists, then* $\int_a^b g(x)\ df(x)$ *exists, and*

$$\int_a^b g(x)\ df(x) = f(b)g(b) - f(a)g(a) - \int_a^b f(x)\ dg(x).$$

(iv) *If $f$ is Riemann integrable on $[a,b]$ and $g'$ is continuous on $[a,b]$, then*

$$\int_a^b f(x)\,dg(x) = \int_a^b f(x)g'(x)\,dx.$$

The proof of Theorem 4.11 can be found in Montgomery and Vaughan [**273**, pp. 487–489] and Apostol [**17**, pp. 142–146 and p. 159]. For our purpose, we only need to express a sum involving arithmetic functions as a Riemann-Stieltjes integral.

Recall that a function $g$ defined on $[a,b]$ is called a *step function* if there is a partition $a = x_1 < x_2 < \cdots < x_n = b$ such that $g$ is a constant on each interval $(x_{i-1}, x_i)$ for $i = 2, 3, \ldots, n$. The *jump* at $x_k$ is defined as

$$\lim_{x\to x_k^+} g(x) - \lim_{x\to x_k^-} g(x) \text{ for } 1 < k < n.$$

The jump at $x_1$ and $x_n$ is defined, respectively, as

$$\lim_{x\to x_1^+} g(x) - g(x_1) \;\text{ and }\; g(x_n) - \lim_{x\to x_n^-} g(x).$$

The following result can be found in Apostol [**17**, pp. 148–149].

**Theorem 4.12.** *Let $g$ be a step function defined on $[a,b]$ with jump $g_k$ at $x_k$, where $x_1, \ldots, x_n$ are as described above. Let $f$ be defined on $[a,b]$ in such a way that both $f$ and $g$ are not discontinuous from the right or from the left at each $x_k$. Then $\int_a^b f(x)\,dg(x)$ exists and*

$$\int_a^b f(x)\,dg(x) = \sum_{k=1}^{n} f(x_k)g_k.$$

Suppose that $f$ is a continuous function defined on $[0,\infty)$. Then the above theorem enable us to express the sum $\sum_{n=1}^{N} a_n f(n)$ in terms of the partial sums $A(x) = \sum_{n\le x} a_n$ and the integral as

$$\sum_{n=1}^{N} a_n f(n) = \int_0^N f(x)\,dA(x). \tag{4.11}$$

The interval of integration in (4.11) can be adjusted as appropriate. The left endpoint can be any number in $[0,1)$ and the right endpoint can be any number in $[N, N+1)$ without affecting the value of the integral. It is often convenient to integrate from $1^-$ to $N$, that is, to consider

$$\lim_{\varepsilon\to 0^+}\int_{1-\varepsilon}^{N} f(x)\,dA(x).$$

So, for example, we have the following equations.

$$\sum_{n=1}^{N} a_n f(n) = \int_0^N f(x)\,dA(x) = \int_{1^-}^{N} f(x)\,dA(x).$$

$$\sum_{n=2}^{N} a_n f(n) = \int_1^N f(x)\,dA(x) = \int_{2^-}^{N} f(x)\,dA(x).$$

$$\sum_{n=3}^{N} a_n f(n) = \int_2^N f(x)\,dA(x) = \int_{3^-}^{N} f(x)\,dA(x).$$

In general, if $x, y \in \mathbb{R}$ and $0 \le y < \lfloor x \rfloor$, then

$$\sum_{y<n\le x} a_n f(n) = \int_y^x f(x)\,dA(x). \tag{4.12}$$

The reader will see the applications of (4.12) throughout this book. For instance, we can now give a short proof of Abel's summation formula as follows:

**Another proof of Theorem 4.10** (the Abel summation formula)**.** By (4.12), (iii) and (iv) of Theorem 4.11, the sum $\sum_{y<n\le x} a_n f(n)$ is equal to

$$\int_y^x f(t)\,dA(t) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,dt,$$

where $A(t) = \sum_{n\le t} a_n$. This gives the proof of this theorem. □

In general, the functions $f$ and g in the integral $\int_a^b f(x)dg(x)$ may be real-valued or complex-valued. We refer the reader to [**273**, Appendix A] and [**17**, Chapter 7] for more properties of the Riemann-Stieltjes integral.

## 4.6. Euler Summation Formula

In estimating a sum, we can use any of the Abel summation formulae, the Euler summation formula, or the Riemann-Steiltjes integral. It usually leads to the same result. So there is no need to remember Euler's formula as we already know the other two. Nevertheless, for completeness and for the learning experience, we use Euler's formula in the next theorem. Recall that for each $x \in \mathbb{R}$, $\lfloor x \rfloor$ is the floor of $x$ and $\{x\}$ is the fractional part of $x$.

**Theorem 4.13.** (Euler's Summation Formula) *Let* $0 < y < x$ *be real numbers and assume that* $f : [y, x] \to \mathbb{R}$ *has a continuous derivative* $f'$ *on* $[y, x]$. *Then*

$$\sum_{y<n\le x} f(n) = \int_y^x f(t)dt + \int_y^x \{t\}f'(t)dt + \{y\}f(y) - \{x\}f(x).$$

**Proof.** We use the Riemann-Steiltjes integral in the form given in (4.12) and then apply (i), (iii), (iv) of Theorem 4.11. Here $a_n = 1$ for all $n$, and so $A(t) = \sum_{n\le t} 1 = \lfloor t \rfloor = t - \{t\}$. Then

$$\begin{aligned}\sum_{y<n\le x} f(n) &= \int_y^x f(t)\, d\lfloor t \rfloor = \int_y^x f(t)\, dt - \int_y^x f(t)\, d\{t\} \\ &= \int_y^x f(t)\, dt + \int_y^x \{t\}f'(t)\, dt - \{x\}f(x) + \{y\}f(y). \qquad \square\end{aligned}$$

Recall from (4.7) that $\sum_{n\le x} \frac{1}{n} = \log x + O(1)$. By applying either Abel's or Euler's summation formula, we can obtain a more accurate formula for the above sum as follows.

**Theorem 4.14.** *For* $x \ge 1$, *we have*

$$\sum_{n\le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right), \tag{4.13}$$

*where* $\gamma$ *is Euler's constant defined by* $\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}dt$. *In addition,* $\gamma$ *is also equal to* $\lim_{x\to\infty} \left(\sum_{n\le x} \frac{1}{n} - \log x\right)$.

**Proof.** By the Euler summation formula, we obtain

$$\sum_{n\le x} \frac{1}{n} = 1 + \sum_{1<n\le x} \frac{1}{n} = 1 + \int_1^x \frac{1}{t}\, dt - \int_1^x \frac{\{t\}}{t^2}\, dt - \frac{\{x\}}{x}.$$

Since $0 \le \frac{\{t\}}{t^2} \le \frac{1}{t^2}$, we see that

$$\int_1^\infty \frac{\{t\}}{t^2}\, dt \text{ converges and } \int_x^\infty \frac{\{t\}}{t^2}\, dt \le \int_x^\infty \frac{1}{t^2}\, dt \ll \frac{1}{x}.$$

Writing $\int_1^x \frac{\{t\}}{t^2}\,dt = \int_1^\infty \frac{\{t\}}{t^2}\,dt - \int_x^\infty \frac{\{t\}}{t^2}\,dt$, the above becomes

$$\sum_{n\le x}\frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right). \tag{4.14}$$

Subtracting both sides of (4.14) by $\log x$ and taking $x \to \infty$, we obtain $\gamma = \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n} - \log x\right)$. This completes the proof. □

For more information about the Euler constant $\gamma$, see Section 4.9. Similar to the previous example, we can also improve the result concerning the sum $\sum_{n\le x}\frac{1}{n^\alpha}$ given in (4.5). An additional term comes from the value of the Riemann zeta function $\zeta$ given by

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{\infty}\frac{1}{n^s} \quad \text{for } s > 1 \text{ and}\\ \zeta(s) &= \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) \quad \text{for } 0 < s < 1.\end{aligned} \tag{4.15}$$

More properties of $\zeta(s)$ will be given in Chapter 8.

**Theorem 4.15.** *For $x \ge 1$, $s > 0$, and $s \ne 1$, we have*

$$\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s}). \tag{4.16}$$

**Proof.** By the Euler summation formula, we obtain

$$\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + c(s) + O(x^{-s}), \tag{4.17}$$

where $c(s) = 1 - \frac{1}{1-s} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,dt$. If $s > 1$, the left-hand side of (4.17) converges to $\zeta(s)$ as $x \to \infty$ while the right-hand side of (4.17) converges to $c(s)$ as $x \to \infty$. So $\zeta(s) = c(s)$ if $s > 1$. If $0 < s < 1$, then (4.17) and (4.15) imply that

$$c(s) = \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) = \zeta(s).$$

So $\zeta(s) = c(s)$ for $0 < s < 1$. This completes the proof. □

## 4.7. Euler-Maclaurin Summation Formula

In order to formulate the Euler-Maclaurin summation formula, we introduce the *Bernoulli polynomials* $B_n(x)$ which are defined inductively by the following conditions: $B_0(x) = 1$, and for $n \geq 1$, we have

$$\frac{d}{dx}B_n(x) = nB_{n-1}(x) \quad \text{and} \quad \int_0^1 B_n(x)\,dx = 0.$$

The *nth Bernoulli number* $B_n$ is defined by $B_n = B_n(0)$. So, for example,

$$\begin{aligned}
&B_0(x) = 1,\ B_1(x) = x - \frac{1}{2},\ B_1(\{x\}) = ((x)),\\
&B_2(x) = x^2 - x + \frac{1}{6},\ B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x,\\
&B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30},\ B_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x,\\
&B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = -\frac{1}{30},\ \text{and } B_5 = 0.
\end{aligned}$$

Equivalently, we can also define $B_n(x)$ and $B_n$ as the coefficients in the series:

$$\begin{aligned}
\sum_{n=0}^{\infty}\frac{B_n(x)z^n}{n!} &= \frac{ze^{xz}}{e^z - 1} \quad \text{for } |z| < 2\pi,\\
\sum_{n=0}^{\infty}\frac{B_n z^n}{n!} &= \frac{z}{e^z - 1} \quad \text{for } |z| < 2\pi.
\end{aligned}$$

In the above series, $z$ is a complex variable and the functions

$$\frac{ze^{xz}}{e^z - 1} \quad \text{and} \quad \frac{z}{e^z - 1}$$

are analytic functions of $z$ in the disk $|z| < 2\pi$. In fact, they are analytic except at the points $z = 2\pi i n$ where $n \in \mathbb{Z} \setminus \{0\}$.

Bernoulli polynomials and Bernoulli numbers have many interesting properties, some of which are given as exercises of Chapters 4 and 8. For now, we only need to know the inductive definition of $B_n$ and $B_n(x)$ to state and prove the following formula.

**Theorem 4.16.** (The Euler-Maclaurin Summation Formula) *Let $y$, $x$ be real numbers, $y < x$, and let $k$ be a positive integer. Assume that $f$ is a function that has continuous derivatives through the kth order on the* *interval* $[y, x]$. *Then*

$$\begin{aligned}\sum_{y<n\le x} f(n) = \int_y^x f(t)dt \\ + \sum_{m=1}^{k} \frac{(-1)^m}{m!}\left(B_m(\{x\})f^{(m-1)}(x) - B_m(\{y\})f^{(m-1)}(y)\right) \\ + \frac{(-1)^{k+1}}{k!}\int_y^x B_k(\{t\})f^{(k)}(t)dt.\end{aligned}$$

*If a and b are integers, the above formula has the form*

$$\begin{aligned}\sum_{n=a}^{b} f(n) = \int_a^b f(t)dt + \frac{1}{2}(f(a) + f(b)) \\ + \sum_{1\le m\le \frac{k}{2}} \frac{B_{2m}}{(2m)!}(f^{(2m-1)}(b) - f^{(2m-1)}(a)) \\ - \frac{1}{(2\ell)!}\int_a^b B_{2\ell}(\{t\})f^{(2\ell)}(t)\,dt, \text{ where } \ell = \left\lfloor \frac{k}{2} \right\rfloor.\end{aligned}$$

**Proof.** We can write

$$\begin{aligned}\sum_{y<n\le x} f(n) = \int_y^x f(t)\,d\lfloor t\rfloor = \int_y^x f(t)\,dt - \int_y^x f(t)\,d\{t\} \\ = \int_y^x f(t)\,dt - \int_y^x f(t)\,dB_1(\{t\}).\end{aligned}$$

The last integral is equal to

$$\begin{aligned}B_1(\{x\})f(x) - B_1(\{y\})f(y) - \int_y^x B_1(\{t\})f'(t)\,dt \\ = B_1(\{x\})f(x) - B_1(\{y\})f(y) - \frac{1}{2}\int_y^x f'(t)dB_2(\{t\}).\end{aligned}$$

It is easy to verify that $B_2(\{t\})$ is continuous on $\mathbb{R}$, differentiable on $\mathbb{R} \setminus \mathbb{Z}$, and $B_2'(\{t\}) = 2B_1(\{t\})$ for $t \in \mathbb{R} \setminus \mathbb{Z}$. Moreover, for $k \ge 3$ $B_k(\{t\})$ is differentiable on $\mathbb{R}$ and satisfies $B_k'(\{t\}) = kB_{k-1}(\{t\})$. See Exercises 4.8.15, 4.8.16, 4.8.17 for an outline of the proof. Then $\int_y^x f'(t)\,dB_2(\{t\})$ is equal to

$$B_2(\{x\})f'(x) - B_2(\{y\})f'(y) - \frac{1}{3}\int_y^x f''(t)\, dB_3(\{t\}).$$

Similarly, the integral $\int_y^x f''(t)dB_3(\{t\})$ is

$$B_3(\{x\})f''(x) - B_3(\{y\})f''(y) - \frac{1}{4}\int_y^x f'''(t)dB_4(\{t\}).$$

Repeating this process to the order $k$ and writing $\int_y^x f^{(k-1)}(t)dB_k(\{t\})$ as

$$B_k(\{x\})f^{(k-1)}(x) - B_k(\{y\})f^{(k-1)}(y) - \int_y^x B_k(\{t\})f^{(k)}(t)dt,$$

we obtain the first formula. If $x \in \mathbb{Z}$, then $\{x\} = 0$, and by Exercises 4.8.12 and 4.8.14, $B_n = B_n(0) = 0$ if $n$ is odd and $n \geq 3$. This leads to the second formula. The details are left as an exercise to the reader. ☐

We can improve the asymptotic formula for the sum $\sum_{m\leq n} \frac{1}{m}$ further as shown in the following example.

**Example 4.17.** For $n \geq 1$, we have

$$\sum_{m\leq n} \frac{1}{m} = \log n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{a(n)}{60n^4} \text{ for some } a(n) \in [0,1]. \tag{4.18}$$

**Solution.** We apply the Euler-Maclaurin summation formula with $f(x) = \frac{1}{x}$, $a = 1$, $b = n$, and $k = 4$. Then the sum on the left-hand side of (4.18) is equal to

$$\begin{aligned} &\int_1^n \frac{1}{t}\, dt + \frac{1}{2}\left(1 + \frac{1}{n}\right) + \frac{B_2}{2!}\left(-\frac{1}{n^2} + 1\right) \\ &\quad + \frac{B_4}{4!}\left(-\frac{6}{n^4} + 6\right) - \int_1^n \frac{B_4(\{t\})}{t^5}\, dt. \end{aligned} \tag{4.19}$$

Recall that $B_4(x) = x^4 - 2x^3 + x^2 - 1/30 = x^2(x-1)^2 - 1/30$, $B_2 = 1/6$, and $B_4 = -1/30$. By a usual technique in calculus, one can find the maximum and minimum values of $B_4(x)$ on $x \in [0,1]$ and obtain

$$-1/30 \leq B_4(x) \leq 1/16 - 1/30 \text{ for all } x \in [0,1].$$

In particular,

$$|B_4(\{t\})| \leq 1/30 \text{ for all } t \text{ and } \int_1^\infty \frac{B_4(\{t\})}{t^5} dt \text{ converges.}$$

Then (4.19) becomes

$$\log n + c + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + \int_n^\infty \frac{B_4(\{t\})}{t^5}\, dt, \tag{4.20}$$

where $c = \frac{1}{2} + \frac{1}{12} - \frac{1}{120} - \int_1^\infty \frac{B_4(\{t\})}{t^5}\, dt$. Let

$$a(n) = 60n^4 \left( \frac{1}{120n^4} + \int_n^\infty \frac{B_4(\{t\})}{t^5} dt \right).$$

Since $|B_4(\{t\})| \leq 1/30$, we obtain

$$\left| \int_n^\infty \frac{B_4(\{t\})}{t^5}\, dt \right| \leq \frac{1}{120n^4} \quad \text{and} \quad 0 \leq a(n) \leq 1.$$

Then (4.20) implies that

$$\sum_{m \leq n} \frac{1}{m} = \log n + c + \frac{1}{2n} - \frac{1}{12n^2} + \frac{a(n)}{60n^4}. \tag{4.21}$$

Comparing (4.21) and Theorem 4.14 and letting $n \to \infty$, we see that $\gamma = c$. This completes the proof. □

**Example 4.18.** For $n \geq 1$, we have

$$\sum_{m \leq n} \log m = n \log n - n + \frac{1}{2} \log n + c + \frac{1}{12n} + \frac{a(n)}{180n^3}$$

where $c = \frac{331}{360} + \frac{1}{4} \int_1^\infty \frac{B_4(\{t\})}{t^4} dt$ and $-1 \leq a(n) \leq 0$.

**Solution.** Applying the Euler–Maclaurin summation formula with $f(t) = \log t$ and $k = 4$, we obtain $\sum_{m \leq n} \log m$ is equal to

$$n \log n - n + \frac{1}{2} \log n + \frac{331}{360} + \frac{1}{12n} - \frac{1}{360n^3} + \frac{1}{4} \int_1^\infty \frac{B_4(\{t\})}{t^4} dt.$$

Writing the integral as $\int_1^\infty \frac{B_4(\{t\})}{t^4} dt - \int_n^\infty \frac{B_4(\{t\})}{t^4} dt$ and using the estimate $|B_4(\{t\})| \leq \frac{1}{30}$ as in the previous exercise, we obtain the desired formula. □

We end this section by giving an important result concerning Bernoulli polynomials. For the proof, see [**18**, Theorem 12.19] or [**273**, pp. 499–500].

**Theorem 4.19.** *Let $x \in \mathbb{R}$. Then the following statements hold.*

(i) *If $x \notin \mathbb{Z}$, then*

$$B_1(\{x\}) = -\frac{1}{\pi}\sum_{m=1}^{\infty}\frac{\sin 2\pi m x}{m}.$$

(ii) *If $n \geq 2$, then*

$$B_n(\{x\}) = -\frac{n!}{(2\pi i)^n}\sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty}\frac{e^{2\pi i m x}}{m^n}.$$

## 4.8. Exercises

4.8.1 Show that the following formulas hold for $x \geq 2$.

(i) $\displaystyle\sum_{n\leq x}\frac{\log n}{n} = \frac{1}{2}(\log x)^2 + A + O\left(\frac{\log x}{x}\right)$, where $A$ is constant.

(ii) $\displaystyle\sum_{2\leq n\leq x}\frac{1}{n\log n} = \log\log x + B + O\left(\frac{1}{x\log x}\right)$, where $B$ is constant.

(iii) $\displaystyle\sum_{n\leq x}(\log n)^2 = x(\log x)^2 - 2x\log x + 2x + O((\log x)^2)$.

4.8.2 Show that for $x \geq 2$,

(i) $\sum_{n\leq x}\log\frac{x}{n} = x + O(\log x)$,

(ii) $\sum_{n\leq x}\left(\log\frac{x}{n}\right)^2 = 2x + O((\log x)^2)$.

In general, prove that

$$\sum_{n\leq x}\left(\log\frac{x}{n}\right)^k = k!\,x + O((\log x)^k) \text{ for } k \geq 1.$$

4.8.3 Show that for $x \geq 2$,

$$\sum_{n\leq x}\log n = x\log x - x + 1 + \theta(x)\log x,$$

where $-\{x\} \leq \theta(x) \leq 1 - \{x\}$.

4.8.4 Let $x_1 = a$, $x_2 = b$, and $x_n = \frac{1}{2}(x_{n-1} + x_{n-2})$ for $n \geq 3$. Show that the series $\sum_{n=1}^{\infty}\frac{(-1)^n x_{2n}}{\log 2n}$ and $\sum_{n=1}^{\infty}\frac{(-1)^n x_{2n-1}}{\log 2n}$ are convergent.

4.8.5 Let $f$ be an arithmetic function such that $\sum_{n\le x} f(n) \ll x$. Prove that $\sum_{n\le x} \frac{f(n)}{n} \ll \log x$ for $x \ge 2$.

4.8.6 Show that for every $x \ge 3$, $\displaystyle\sum_{n\le x} \frac{1}{3 + n\log n} \ll \log\log x$.

4.8.7 Show that $e$ is irrational.

4.8.8 Recall that the $p$-adic valuation of $n!$ is given by

$$v_p(n!\,) = \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of digits of $n$ in base $p$. Prove the following statements.

(i) For every prime $p$, $\displaystyle\lim_{n\to\infty} \frac{v_p(n!\,)}{n} = \frac{1}{p-1}$.

(ii) If $n \in \mathbb{N}$ and $p$ is a prime, then $p^{v_p(n!)} \le 2^{n-1}$.

4.8.9 Prove that $e\left(\frac{n}{e}\right)^n < n! < en\left(\frac{n}{e}\right)^n$ for every $n \ge 2$.

4.8.10 Show that if

$$\left(\sum_{n=0}^{\infty} \frac{a_n z^n}{n!}\right)\left(\sum_{n=0}^{\infty} \frac{b_n z^n}{n!}\right) = \sum_{n=0}^{\infty} \frac{c_n z^n}{n!},$$

then $c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$ for every $n \ge 0$.

In Exercises 4.8.11 to 4.8.13, assuming the Bernoulli polynomials $B_n(x)$ and the Bernoulli numbers $B_n$ satisfy

$$\sum_{n=0}^{\infty} \frac{B_n(x) z^n}{n!} = \frac{z e^{xz}}{e^z - 1} \quad \text{for } |z| < 2\pi,$$

$$\sum_{n=0}^{\infty} \frac{B_n z^n}{n!} = \frac{z}{e^z - 1} \quad \text{for } |z| < 2\pi,$$

prove the following statements and deduce the inductive definition of $B_n(x)$.

4.8.11 Show that $B_0(x) = 1$ and for $n \ge 1$, $B_n(x)$ is a polynomial of degree $n$ given by

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}.$$

4.8.12 Prove the following statements.

(i) $B_n(x+1) - B_n(x) = nx^{n-1}$ for $n \geq 1$,
(ii) $B_n(1) = B_n(0)$ for all $n \geq 2$,
(iii) $B_n = \sum_{k=0}^{n} \binom{n}{k} B_k$ for $n \geq 2$.

4.8.13 Deduce the inductive definition of $B_n(x)$ that $B_0(x) = 1$ and for $n \geq 1$,

$$\frac{d}{dx} B_n(x) = nB_{n-1}(x) \quad \text{and} \quad \int_0^1 B_n(x)\,dx = 0.$$

4.8.14 Prove that for every $n \geq 0$ and $x \in \mathbb{R}$, we have

$$B_n(1-x) = (-1)^n B_n(x) \quad \text{and} \quad B_{2n+1}(1/2) = 0.$$

In Exercises 4.8.15 to 4.8.17, use the inductive definition of $B_n(x)$ to prove the following results.

4.8.15 Show that, for each $n \geq 0$, $B_n(x)$ is a polynomial of degree $n$.

4.8.16 Show that $B_n(1) = B_n(0)$ for all $n \geq 2$ and $B_n'(1) = B_n'(0)$ for all $n \geq 3$.

4.8.17 Let $n \geq 2$. Prove the following statements.
(i) The function $x \mapsto B_n(\{x\})$ has period one.
(ii) The function $x \mapsto B_n(\{x\})$ is continuous on $\mathbb{R}$.
(iii) If $n \geq 3$, then the function $x \mapsto B_n(\{x\})$ is differentiable on $\mathbb{R}$.

4.8.18 Suppose that $g : [1,\infty) \to \mathbb{R}$ is bounded and integrable on every bounded subinterval of $[1,\infty)$ and $g(x) = o(1)$ as $x \to \infty$. Show that

$$\int_1^x g(t)dt = o(x) \quad \text{as } x \to \infty.$$

4.8.19 Let $f, g : [1,\infty) \to \mathbb{R}$ be bounded and integrable on every bounded subinterval of $[1,\infty)$, $f(x) > 0$ for all $x$, and $g(x) = o(f(x))$ as $x \to \infty$. Suppose that $\int_1^x f(t)dt \to \infty$ as $x \to \infty$. Show that

$$\int_1^x g(t)dt = o\left(\int_1^x f(t)dt\right) \quad \text{as } x \to \infty.$$

## 4.9. Notes

Bachmann [**24**, p. 401] and Landau [**240**, p. 61] introduced, respectively, the big $O$ and the little $o$; Hardy [**171**] was the first to use the notations

$f \asymp g$ and $f \sim g$; Hardy and Littlewood [**174**, p. 225] invented the omega $\Omega_R$, $\Omega_L$ notations; and Ingham [**209**] then replaced $\Omega_R$ and $\Omega_L$ by $\Omega_+$ and $\Omega_-$, respectively. As mentioned earlier, the notations $\ll$ and $\gg$ are due to Vinogradov. We give the definitions of the omega $\Omega$, $\Omega_+$, $\Omega_-$, $\Omega_\pm$ notations below. As usual, let $a \geq 1$, $f, g : [a, \infty) \to \mathbb{R}$ and $g(x) > 0$ for all $x \geq a$. Then

$$\begin{aligned} f(x) = \Omega(g(x)) \text{ as } x \to \infty \;&\Leftrightarrow \limsup_{x\to\infty} |f(x)/g(x)| > 0, \\ f(x) = \Omega_+(g(x)) \text{ as } x \to \infty \;&\Leftrightarrow \limsup_{x\to\infty} f(x)/g(x) > 0, \\ f(x) = \Omega_-(g(x)) \text{ as } x \to \infty \;&\Leftrightarrow \liminf_{x\to\infty} f(x)/g(x) < 0, \\ f(x) = \Omega_\pm(g(x)) \text{ as } x \to \infty \;&\Leftrightarrow f(x) = \Omega_+(g(x)) \\ &\qquad \text{and } f(x) = \Omega_-(g(x)). \end{aligned}$$

Again, these notations are standard in analytic number theory but they may have different meaning in other subjects.

Euler defined the constant $\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}dt \approx 0.5772156649\ldots$ given in Theorem 4.14 which he denoted by $C$. Mascheroni replaced $C$ by $\gamma$, and so $\gamma$ is sometimes called the Euler-Mascheroni constant. The constants $e$, $\pi$, $\gamma$ appear frequently in number theory, see for example the theorems and exercises in Chapters 4 and 5. However, while the irrationality of $e$ and $\pi$ is known, that of $\gamma$ is just a conjecture and a proof seems beyond our reach. The approximation of $\gamma$ is also more difficult than that of $\pi$ and $e$ since the convergence rate is slow. Here are some estimates, series, or products involving $\gamma$ which can be found in [**122**, pp. 29–31]:

$$\begin{aligned} \frac{1}{2(n+1)} < \sum_{k\leq n} \frac{1}{k} - \log n - \gamma < \frac{1}{2n}, \\ \gamma = \sum_{m=2}^{\infty} \frac{(-1)^m}{m} \sum_{k=1}^{\infty} \frac{1}{k^m}, \quad \text{and} \\ \frac{6e^\gamma}{\pi^2} = \lim_{n\to\infty} \frac{1}{\log n} \prod_{p\leq n} \left(1 + \frac{1}{p}\right). \end{aligned}$$

For more information on $\gamma$ and other mathematical constants, we refer the reader to the book by Finch [**122**].

By Exercise 4.8.8, it follows that $\lim_{n\to\infty}(v_2(n!)/v_3(n!)) = 2$ so $v_2(n!)/v_3(n!)$ is arbitrarily close to 2 but it is not known whether there are infinitely many $n \in \mathbb{N}$ such that $v_2(n!) = 2v_3(n!)$. Since $v_p(n!) = (n - s_p(n))/(p-1)$, this is equivalent to determining if there are infinitely many $n$ such that $s_2(n) = s_3(n)$. Here $s_b(n)$ is the sum of digits of $n$ when $n$ is written in base $b$. By using a computer, we can obtain the positive integers $n \le 100$ satisfying $s_2(n) = s_3(n)$, namely, $n = 1, 6, 7, 10, 11, 12, 13, 18, 19, 21, 36, 37, 46, 47, 58, 59, 60, 61, 86, 92$. For a longer list of $n$, see the sequence A037301 in OEIS.

By using a simple estimate for the sum $\sum_{m \le n} \log m$, one can obtain the result given in Exercise 4.8.9: $e\,(n/e)^n < n! < en\,(n/e)^n$ for all $n \ge 2$. The well-known Stirling formula states that $n!$ is asymptotic to $\sqrt{2\pi n}\,(n/e)^n$ as $n \to \infty$. Burnside [**68**] improved it to

$$n! \sim \sqrt{2\pi}\left(\frac{n+\frac{1}{2}}{e}\right)^{n+\frac{1}{2}}.$$

Ramanujan also made some contributions to the study of $n!$. For instance, he [**338**, p. 339] gave the formula

$$\Gamma(x+1) = \sqrt{\pi}\left(\frac{x}{e}\right)^x \left(8x^3 + 4x^2 + x + \frac{\theta_x}{30}\right)^{\frac{1}{6}}, \tag{4.22}$$

where $\frac{3}{10} < \theta_x < 1$ and $\theta_x \to 1$ as $x \to \infty$. So if $x = n$ is a positive integer, then (4.22) implies

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \left(1 + \frac{1}{12n} + \frac{1}{8n^2} + \frac{\theta_n}{240n^3}\right)^{\frac{1}{6}}. \tag{4.23}$$

Ramanujan [**338**, p. 326] also showed that for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that if $n \ge N$, then

$$c^{\frac{(1-\varepsilon)n}{\log n}} < d(n!) < c^{\frac{(1+\varepsilon)n}{\log n}}, \tag{4.24}$$

where $c$ is a constant given by $c = \prod_{k=1}^{\infty}\left(1 + \frac{1}{k}\right)^{\frac{1}{k}}$. In other words,

$$\lim_{n\to\infty} \frac{(\log n)\log d(n!)}{(\log c)n} = 1.$$

In fact, Ramanujan proved a more precise version of (4.24) in his paper [**336**, Equations 265–267], [**339**, p. 127], namely,

$$d(n!) = c^{\frac{n}{\log n} + O\left(\frac{n}{(\log n)^2}\right)} \quad \text{for } n \ge 2. \tag{4.25}$$

For a lot more details on the work of Ramanujan, we refer the reader to his collection [**338–340**] and his notebooks which are collected and explained by Berndt [**43–47**] and by Andrews and Berndt [**12–15**]. After Ramanujan, many other results on $n!$ have been discovered. Here we mention a few. Hirschhorn and Villarino [**187**] gave an improvement on $\theta_n$ in (4.23) and a stronger inequality than Exercise 4.8.9. For instance, they [**187**] showed that

$$1-\frac{11}{8n}+\frac{79}{112n^2}<\theta_n<1-\frac{11}{8n}+\frac{79}{112n^2}+\frac{20}{33n^3},\quad \text{and}$$
$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n<n!\leq\sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}\quad \text{for } n\geq 1.$$

Erdös, Graham, Ivić, and Pomerance [**117**, p. 339] improved (4.25) to the following form: for any fixed integer $K\geq 0$, we have

$$d(n!)=\exp\left(\frac{n}{\log n}\sum_{k=0}^{K}\frac{c_k}{(\log n)^k}+O\left(\frac{n}{(\log n)^{K+2}}\right)\right),$$

where the $c_k$ are explicitly given constants and in particular,

$$c_0=\sum_{k=2}^{\infty}\frac{\log k}{k(k-1)}\approx 1.25775.$$

We remark that if $c$ is the constant in (4.24), then $\log c=c_0$.

Other problems related to the divisor function can be found in, for instance, Andrews and Berndt [**15**, Chapter 1], Berndt, Kim, and Zaharescu [**48–50**], Berndt and Pongsriiam [**51**], Liu, Shparlinski, and Zhang [**247**] and Pongsriiam and Vaughan [**327–329**]. Diophantine equations involving arithmetic of factorials were also investigated by some mathematicians. For example, Luca [**250**] obtained all solutions to the equations $\varphi(n!)=m!$, $\sigma(n!)=m!$, and $d(n!)=m!$, where $\varphi$, $\sigma$, $d$ are, respectively, the Euler function, the sum of divisor function, and the divisor function. This study was extended by Baczkowski, Filaseta, Luca, and Trifonov [**27**], where the functions involved are the same but there are more variables in the equation. Luca and Shparlinski [**253**] also considered this type of equation but $\varphi$, $\sigma$, $d$ are replaced by the Ramanujan $\tau$ function. In addition, Pongsriiam [**320**], among other things, determined all positive integers $m, n, k$ satisfying $z(m!)=a^k n!$ or $b^k z(m!)=n!$, where the function $z$ is the order of appearance in the Fibonacci sequence introduced in the notes of Chapter 2 and $1\leq a,b\leq 10$ are fixed positive integers. For other articles on arithmetic functions of factorials and of other integer sequences, we refer the reader to Hassani [**182**], Luca [**249**], Sahukar and Panda [**351**], Luca and Young [**254**], Bugeaud, Luca, Mignotte, and Siksek [**64**], Jaidee and Pongsriiam [**216**], and Pongsriiam [**321**].

## Chapter 5

# Arithmetic Functions II

### 5.1. Introduction

Previously, we obtained various identities for the arithmetic functions $d$, $\varphi$, $\sigma$, $\mu$, $e$, $N$, and $\Lambda$. In this chapter, we give some analytic results concerning these functions and their combinations. Suppose $f$ is an arithmetic function. Then some of the following questions may be considered. Does the limit $\lim_{n\to\infty} f(n)$ exist? If it exists, what is its value? If it does not exist, what is the value of $\liminf_{n\to\infty} f(n)$ and $\limsup_{n\to\infty} f(n)$? Can we obtain some nontrivial bounds for $f(n)$? Can we find an asymptotic formula for the sum $\sum_{n\le x} f(n)$?

Consider, for example, the divisor function. It is easy to see that $d(n) = 2$ for infinitely many $n$ (when $n$ is prime) and $d(n)$ can be arbitrarily large (for instance when $n$ is a product of $k$ distinct primes and $k$ is large). Therefore

$$\liminf_{n\to\infty} d(n) = 2, \quad \limsup_{n\to\infty} d(n) = \infty,$$

and it is interesting to find a nontrivial upper bound $g(n)$ for $d(n)$ such that

$$0 < \limsup_{n\to\infty} d(n)/g(n) < \infty.$$

Similarly, for the Euler function, we have

$$\lim_{n\to\infty} \varphi(n) = +\infty, \quad \limsup_{n\to\infty} \varphi(n)/n = 1,$$

and if $f(n) = e^{-\gamma} n / \log\log n$ and $\gamma$ is Euler's constant, then

$$\liminf_{n\to\infty} \varphi(n)/f(n) = 1.$$

We explain more about this in Section 5.4. Since $d(n)$ and the values of many arithmetic functions oscillate considerably as $n$ increases, it is of interest to study their mean values or average orders (see Definition 5.1). For example, by calculating the partial sum $\sum_{n\le x} \omega(n)$ and using Turán's method, one can obtain that almost all positive integers $n$ have $\log\log n$ prime factors. More precisely, if $\varepsilon > 0$ is given, then

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \in \mathbb{N} \mid 2 \le n \le x \text{ and } \left| \frac{\omega(n)}{\log\log n} - 1 \right| < \varepsilon \right\} = 1.$$

The precise definitions of mean value, average order, extremal order, and normal order are as follows.

**Definition 5.1.** Let $f$ be an arithmetic function. Then the *mean value* (or the *average value*) of $f$ over the interval $[1, x]$ is defined to be

$$F(x) = \frac{1}{x} \sum_{n\le x} f(n).$$

If $\lim_{x\to\infty} F(x)$ exists, then the limit is called the *asymptotic mean value* of $f$. In addition, if $g$ is a monotone function such that

$$F(x) \sim \frac{1}{x} \sum_{n\le x} g(n),$$

then we say that $g(n)$ is an *average order* of $f(n)$.

If $P$ is a mathematical property, then the statement “$g$ is eventually $P$” means that $g(n)$ satisfies $P$ for all large values of $n$. For example, $g$ is eventually positive means that there exists $N \in \mathbb{N}$ such that $g(n) > 0$ for all $n \ge N$. We use the term “eventually $P$” in the following definitions.

**Definition 5.2.** Suppose that $g$ is eventually positive and eventually monotone. Then $g$ is a *maximal order* of $f$ if

$$\limsup_{n\to\infty} f(n)/g(n) = 1,$$

and that $g$ is a *minimal order* of $f$ if $\liminf_{n\to\infty} f(n)/g(n) = 1$.

**Definition 5.3.** Suppose that $g$ is eventually positive and eventually monotone. Then $f(n)$ has *normal order* $g(n)$ if for every $\varepsilon > 0$,

$$\lim_{x\to\infty} \left( \frac{1}{x} \# \{ n \le x : |f(n) - g(n)| < \varepsilon g(n) \} \right) = 1.$$

In other words, for each $\varepsilon > 0$, the number of positive integers $n \le x$ such that $|f(n) - g(n)| \ge \varepsilon g(n)$ is $o(x)$. In this case, we also write, in a similar way as in measure theory, $f(n) = (1 + o(1))g(n)$ a.e.

We give mean values and average orders for the functions $d$, $\varphi$, $\sigma$, $\omega$, and $\Omega$ in Section 5.2 and then provide extremal orders of these functions in Section 5.4. Normal orders are discussed in Section 5.5. It is desirable that the function $g$ in Definitions 5.1 to 5.3 should be an elementary function which is monotone and positive, but for flexibility, some of these conditions are sometimes removed from the definition. If $g(n) \neq 0$, then the condition $|f(n) - g(n)| < \varepsilon g(n)$ may be written as $|f(n)/g(n) - 1| < \varepsilon$ which gives a sense of $f(n) = g(n)$ for almost all $n$. We remark that the problem of calculating the partial sum $\sum_{n\le x} f(n)$ and the question of finding the asymptotic mean value of $f(n)$ over $[1, x]$ may be different. For instance, it is known that

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \mu(n) = 0,$$

and so the asymptotic mean value of $\mu(n)$ is zero but the asymptotic estimate for the partial sum $\sum_{n\le x} \mu(n)$ is not known and it seems extremely difficult. We will say something more about this later. For now, let us proceed to the next section on average orders.

## 5.2. Average Orders

We first calculate the partial sum of the divisor function by a simple method of interchanging the order of summation. We have

$$\begin{aligned}
\text{(5.1)} \qquad \sum_{n\le x} d(n) &= \sum_{n\le x}\sum_{d\mid n} 1 = \sum_{d\le x}\sum_{\substack{n\le x\\ d\mid n}} 1 \\
&= \sum_{d\le x} \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d\le x} \left( \frac{x}{d} + O(1) \right) \\
&= x \sum_{d\le x} \frac{1}{d} + O(x) \\
\text{(5.2)} \qquad &= x \log x + O(x).
\end{aligned}$$

So

$$\frac{1}{x}\sum_{n\le x} d(n) = \log x + O(1) \sim \log x \sim \frac{1}{x}\sum_{n\le x}\log n,$$

which gives $\log n$ as an average order of $d(n)$. The reader who is not familiar with changing the order of summation in (5.1) should recall this technique from a calculus course. We can obtain (5.1) directly from the equality of the sets

$$\{(n,d)\in\mathbb{N}\times\mathbb{N} \mid n\le x \wedge d\mid n\} \text{ and}$$
$$\{(n,d)\in\mathbb{N}\times\mathbb{N} \mid d\le x \wedge n\le x \wedge d\mid n\},$$

or we can view it geometrically on the $(n,d)$-plane in a similar way as we do in calculus. Suppose

$$D = \{(x,y)\in\mathbb{R}^2 \mid 0\le x\le 5 \text{ and } 0\le y\le x^2\}$$

and $f : \mathbb{R}^2 \to \mathbb{R}$ is a continuous function. Then

$$\iint\limits_D f dA = \int_0^5\int_0^{x^2} f(x,y)dydx.$$

We cannot simply change the order of the integral as $\int_0^{x^2}\int_0^5 f(x,y)dxdy$. In fact, the set $D$ is equal to

$$\{(x,y)\in\mathbb{R}^2 \mid 0\le y\le 25 \text{ and } \sqrt{y}\le x\le 5\}$$

and another correct form is

$$\iint\limits_D f dA = \int_0^{25}\int_{\sqrt{y}}^5 f(x,y)dxdy.$$

Since this technique is used often, we show the calculation again using a different notation to help the reader get more familiar with it. We have

$$\sum_{n\le x} d(n) = \sum_{n\le x}\sum_{d\mid n} 1.$$

Since $d \mid n$, we can write $n = dk$. So the above sum can be written as

$$\sum_{dk\le x} 1.$$

This can be viewed as a sum extended over lattice points $(d, k)$ with $dk \leq x$ in the $(d, k)$-plane. Next, we fix $d \leq x$ and sum over $k \leq \frac{x}{d}$ to obtain

$$\sum_{dk\leq x} 1 = \sum_{d\leq x} \sum_{k\leq \frac{x}{d}} 1 = \sum_{d\leq x} \left\lfloor \frac{x}{d} \right\rfloor = x\log x + O(x),$$

which is the same as (5.2). It is also possible to improve (5.2) by using Dirichlet's hyperbola method and we will do this in the next section. Now let us summarize the above technique in the following theorem.

**Theorem 5.4.** *Let* $F(x) = \sum_{n\leq x} f(n)$ *for every* $x \geq 1$. *Then*

$$\sum_{n\leq x} \sum_{d|n} f(d) = \sum_{d\leq x} f(d) \left\lfloor \frac{x}{d} \right\rfloor = \sum_{k\leq x} F\left(\frac{x}{k}\right).$$

**Proof.** We have

$$\sum_{n\leq x} \sum_{d|n} f(d) = \sum_{dk\leq x} f(d).$$

Fixing $d \leq x$ and summing over $k \leq \frac{x}{d}$ gives

$$\sum_{dk\leq x} f(d) = \sum_{d\leq x} f(d) \sum_{k\leq \frac{x}{d}} 1 = \sum_{d\leq x} f(d) \left\lfloor \frac{x}{d} \right\rfloor.$$

On the other hand, if we fix $k \leq x$ and sum over $d \leq \frac{x}{k}$, we obtain

$$\sum_{dk\leq x} f(d) = \sum_{k\leq x} \sum_{d\leq \frac{x}{k}} f(d) = \sum_{k\leq x} F\left(\frac{x}{k}\right).$$

This completes the proof. □

Next, we apply this method to obtain the asymptotic formulas for the partial sums of $\sigma(n)$ and $\varphi(n)$. For the sum $\sum_{n\leq x} \sigma_\alpha(n)$, see Exercise 5.6.3.

**Theorem 5.5.** $\displaystyle\sum_{n\leq x} \sigma(n) = \frac{\pi^2}{12} x^2 + O(x\log x)$ *for* $x \geq 2$.

**Proof.** We have $\sum_{n\leq x} \sigma(n) = \sum_{n\leq x} \sum_{d|n} d = \sum_{dk\leq x} d$. Now we have two choices. One is to sum $d$ and then $k$. The other is to sum $k$ and then $d$. Which way gives a better result? In general, we can try both and see what happens. In this proof, we sum the larger one first. Here $d$ is larger than or equal to 1. So we write

(5.3)

$$\sum_{dk\le x} d = \sum_{k\le x}\sum_{d\le\frac{x}{k}} d = \sum_{k\le x}\frac{1}{2}\left\lfloor\frac{x}{k}\right\rfloor\left(\left\lfloor\frac{x}{k}\right\rfloor+1\right) = \frac{1}{2}\sum_{k\le x}\left(\frac{x^2}{k^2}+O\left(\frac{x}{k}\right)\right).$$

By distributing the sum and recalling that $\sum_{k=1}^{\infty}\frac{1}{k^2}=\frac{\pi^2}{6}$, the above is

$$\begin{aligned}\frac{1}{2}x^2\sum_{k\le x}\frac{1}{k^2}+O\left(x\sum_{k\le x}\frac{1}{k}\right) &= \frac{1}{2}x^2\left(\sum_{k=1}^{\infty}\frac{1}{k^2}-\sum_{k>x}\frac{1}{k^2}\right)+O(x\log x)\\ &= \frac{\pi^2}{12}x^2+O(x\log x),\end{aligned}$$

which gives the desired result. ☐

**Remark 5.6.** Let us consider (5.3) again. If we sum $k$ and then $d$, we will get a trivial result as follows.

$$\begin{aligned}\sum_{dk\le x} d = \sum_{d\le x} d\sum_{k\le\frac{x}{d}}1 &= \sum_{d\le x} d\left\lfloor\frac{x}{d}\right\rfloor = \sum_{d\le x} d\left(\frac{x}{d}+O(1)\right)\\ &= x\lfloor x\rfloor + O\left(\sum_{d\le x} d\right) \ll x^2.\end{aligned}$$

This means that $\sum_{n\le x}\sigma(n)=O(x^2)$, which is correct but gives less information than Theorem 5.5.

In Chapter 8, we will show that for every $s>1$, we have

$$\left(\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}\right)\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right)=1.$$

Since $\sum_{n=1}^{\infty}1/n^2=\pi^2/6$, we see that $\sum_{n=1}^{\infty}\mu(n)/n^2=6/\pi^2$. We give an outline in Exercise 5.6.2 on how to obtain

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=\frac{6}{\pi^2}$$

without using the Euler product formula or any knowledge from Chapter 8. We need to use this fact to prove the following theorem.

**Theorem 5.7.** $\displaystyle\sum_{n\le x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x)$ *for* $x\ge 2$.

**Proof.** We begin by writing $\varphi(n)$ as a divisor sum: $\varphi(n) = n\sum_{d|n}\frac{\mu(d)}{d}$. Then

$$\sum_{n\le x}\varphi(n) = \sum_{n\le x}\left(n\sum_{d|n}\frac{\mu(d)}{d}\right) = \sum_{dk\le x}(dk)\left(\frac{\mu(d)}{d}\right) = \sum_{dk\le x}k\mu(d).$$

The order of summation here should be chosen as

$$\sum_{d\le x}\mu(d)\sum_{k\le\frac{x}{d}}k.$$

The reason for this is that we do not know the formula for $\sum_{n\le x}\mu(n)$, so writing

$$\sum_{dk\le x}k\mu(d) = \sum_{k\le x}k\sum_{d\le\frac{x}{k}}\mu(d)$$

leads to a difficult calculation (see also the notes in Section 5.7 for more details). Then we obtain

$$\begin{aligned}\sum_{dk\le x}k\mu(d) &= \sum_{d\le x}\mu(d)\sum_{k\le\frac{x}{d}}k = \sum_{d\le x}\mu(d)\left(\frac{1}{2}\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)\right)\\ &= \frac{1}{2}\sum_{d\le x}\mu(d)\left(\frac{x^2}{d^2}+O\left(\frac{x}{d}\right)\right)\\ &= \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2}+O\left(x\sum_{d\le x}\frac{1}{d}\right)\\ &= \frac{x^2}{2}\left(\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}-\sum_{d>x}\frac{\mu(d)}{d^2}\right)+O(x\log x)\\ &= \frac{3}{\pi^2}x^2+O(x\log x).\end{aligned}$$

In the last equality, we use the fact that $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$. □

To calculate the partial sum $\sum_{n\le x}\omega(n)$, we use the fact that the number of primes $p\le x$ is $O(x/\log x)$ and that

$$\sum_{p\le x}\frac{1}{p} = \log\log x + b + O\left(\frac{1}{\log x}\right),$$

where $b$ is a constant, which will be proved in the next chapter. See also Exercise 5.6.18 for an outline of another proof of Theorems 5.8 and 5.9. For now, we assume this result and prove the following theorem.

**Theorem 5.8.** *For $x \geq 2$, we have*

$$\sum_{n \leq x} \omega(n) = x \log\log x + bx + O\left(\frac{x}{\log x}\right),$$

*where $b$ is a constant.*

**Proof.** As usual, let $p$ denote a prime. We write $\omega(n) = \sum_{p|n} 1$ and change the order of summation to obtain

$$\sum_{n \leq x} \omega(n) = \sum_{p \leq x} \sum_{\substack{n \leq x \\ p|n}} 1 = \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor = x \sum_{p \leq x} \frac{1}{p} + O\left(\frac{x}{\log x}\right).$$

Substituting the formula for $\sum_{p \leq x} \frac{1}{p}$ as mentioned above, we obtain the desired formula. ☐

**Theorem 5.9.** *For $x \geq 2$, we have*

$$\sum_{n \leq x} \Omega(n) = x \log\log x + cx + O\left(\frac{x}{\log x}\right),$$

*where $c = b + \sum_p \frac{1}{p(p-1)}$ and $b$ is the constant given in Theorem* 5.8.

**Proof.** We write $\Omega(n) = \sum_{p^a|n} 1$ and change the order of summation to obtain

$$\sum_{n \leq x} \Omega(n) = \sum_{p^a \leq x} \left\lfloor \frac{x}{p^a} \right\rfloor = \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor + \sum_{\substack{p^a \leq x \\ a \geq 2}} \left\lfloor \frac{x}{p^a} \right\rfloor. \tag{5.4}$$

The first sum on the right-hand side of (5.4) is $\sum_{n \leq x} \omega(n)$ as shown in the proof of the previous theorem. For the second sum, we write $\lfloor x/p^a \rfloor = x/p^a + O(1)$. The error $O(1)$ contributes to

$$\sum_{2 \leq a \leq \frac{\log x}{\log 2}} \sum_{p \leq x^{\frac{1}{a}}} 1 \ll \sum_{2 \leq a \leq \frac{\log x}{\log 2}} \pi\left(x^{\frac{1}{a}}\right) \ll (\log x)\, \pi\left(\sqrt{x}\right) \ll \sqrt{x}.$$

Therefore

$$\sum_{\substack{p^a \leq x \\ a \geq 2}} \left\lfloor \frac{x}{p^a} \right\rfloor = x \sum_{\substack{p^a \leq x \\ a \geq 2}} \frac{1}{p^a} + O\left(\sqrt{x}\right). \tag{5.5}$$

The main term on the right-hand side of (5.5) is

$$x \sum_{a=2}^{\infty} \sum_{p^a \leq x} \frac{1}{p^a} = x \sum_{a=2}^{\infty} \sum_{p} \frac{1}{p^a} - x \sum_{a=2}^{\infty} \sum_{p^a > x} \frac{1}{p^a}. \tag{5.6}$$

The first sum on the right-hand side of (5.6) is $\sum_p \frac{1}{p(p-1)}$. For each $p \leq \sqrt{x}$, let $A = \left\lfloor \frac{\log x}{\log p} \right\rfloor + 1$. Then $p^{A-1} \leq x < p^A$ and the second sum on the right-hand side of (5.6) is

$$\begin{aligned}\sum_p \sum_{\substack{a\geq 2\\ a>\frac{\log x}{\log p}}} \frac{1}{p^a} &= \sum_{p>\sqrt{x}} \sum_{a=2}^{\infty} \frac{1}{p^a} + \sum_{p\leq\sqrt{x}} \sum_{a>\frac{\log x}{\log p}} \frac{1}{p^a} \\ &\ll \sum_{n>\sqrt{x}} \frac{1}{n(n-1)} + \sum_{p\leq\sqrt{x}} \frac{1}{p^{A-1}(p-1)} \\ &\ll \sum_{n>\sqrt{x}} \frac{1}{n^2} + \sum_{p\leq\sqrt{x}} \frac{1}{p^A} \\ &\ll \frac{1}{\sqrt{x}} + \frac{\sqrt{x}}{\log x} \cdot \frac{1}{x} \ll \frac{1}{\sqrt{x}}.\end{aligned}$$

So the right-hand side of (5.6) is $x \sum_p \frac{1}{p(p-1)} + O\left(\sqrt{x}\right)$. This implies the desired result. ☐

By Theorems 5.5, 5.7, 5.8, and 5.9, we see that the mean values of $\sigma(n)$, $\varphi(n)$, $\omega(n)$, and $\Omega(n)$ over $[1, x]$ are asymptotic to $\pi^2 x/12$, $3x/\pi^2$, $\log\log x$, and $\log\log x$, respectively. In addition, since

$$\sum_{n\leq x} \sigma(n) \sim \sum_{n\leq x} \frac{\pi^2}{6} n \text{ and } \sum_{n\leq x} \varphi(n) \sim \sum_{n\leq x} \frac{6}{\pi^2} n,$$

the average orders of $\sigma(n)$ and $\varphi(n)$ are $\frac{\pi^2}{6}n$ and $\frac{6}{\pi^2}n$, respectively. Similarly, the average order of both $\omega(n)$ and $\Omega(n)$ is $\log\log n$. The estimate for the partial sum $\sum_{n\leq x} \Lambda(n)$ is more difficult and will be given in Chapters 6 and 9 but the answer is that $\sum_{n\leq x} \Lambda(n) \sim x$. So 1 is an average order $\Lambda(n)$. The asymptotic estimate for the sum $\sum_{n\leq x} \mu(n)$ is not known and seems beyond our reach, see the notes in Section 5.7 for more details.

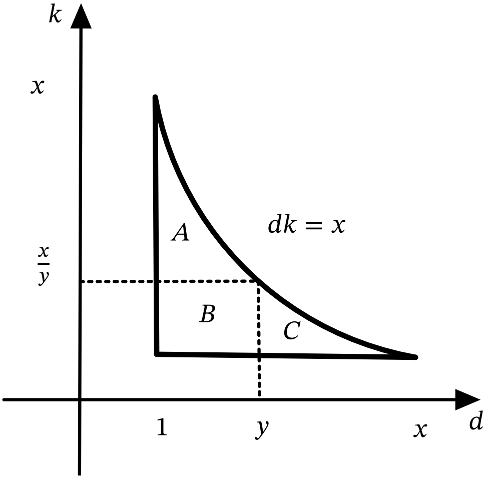
## 5.3. Dirichlet's Hyperbola Method

As mentioned earlier, we can improve (5.2) by using the Dirichlet hyperbola method as shown in the next theorem.

**Theorem 5.10.** (Dirichlet's Hyperbola Method) *Let $f$ and $g$ be arithmetic functions. For any $y > 0$, we have*

$$\sum_{n\le x}(f*g)(n) = \sum_{dk\le x} f(d)g(k) =$$

$$\sum_{d\le y} f(d)\sum_{k\le \frac{x}{d}} g(k) + \sum_{k\le \frac{x}{y}} g(k)\sum_{d\le \frac{x}{k}} f(d) - \left(\sum_{k\le \frac{x}{y}} g(k)\right)\left(\sum_{d\le y} f(d)\right).$$



**Proof.** If $y < 1$ or $y > x$, the result is obvious. So assume that $1 \le y \le x$. The first equality $\sum_{n\le x}(f*g)(n) = \sum_{dk\le x} f(d)g(k)$ follows from the definition of $f*g$. So we only need to prove the second equality. The sum $\sum_{dk\le x} f(d)g(k)$ is extended over all pairs $(d,k)$ in the region $A\cup B\cup C$ in the picture. The right-hand side is the sum over all pairs $(d,k)$ in the region $A\cup B$, $B\cup C$, and $B$, respectively. This implies the desired result.

*Alternative proof.* We can also directly calculate the sum as follows.

$$\begin{aligned}\sum_{dk\le x} f(d)g(k) &= \sum_{\substack{dk\le x\\ d\le y}} f(d)g(k) + \sum_{\substack{dk\le x\\ d>y}} f(d)g(k)\\ &= \sum_{d\le y} f(d)\sum_{k\le \frac{x}{d}} g(k) + \sum_{k<\frac{x}{y}} g(k)\sum_{y<d\le \frac{x}{k}} f(d).\end{aligned}$$

Then we write the second sum as

$$\begin{aligned}\sum_{k<\frac{x}{y}} g(k)\left(\sum_{d\le\frac{x}{k}} f(d)-\sum_{d\le y} f(d)\right)\\ &=\sum_{k<\frac{x}{y}} g(k)\sum_{d\le\frac{x}{k}} f(d)-\left(\sum_{k<\frac{x}{y}} g(k)\right)\left(\sum_{d\le y} f(d)\right)\\ &=\sum_{k\le\frac{x}{y}} g(k)\sum_{d\le\frac{x}{k}} f(d)-\left(\sum_{k\le\frac{x}{y}} g(k)\right)\left(\sum_{d\le y} f(d)\right).\end{aligned}$$

This leads to the desired formula. □

Applying Dirichlet's hyperbola method to the partial sum of $d(n)$, we can now improve (5.2) as follows.

**Theorem 5.11.** *We have*

$$\sum_{n\le x} d(n) = x\log x + (2\gamma-1)x + O(\sqrt{x}),$$

*where $\gamma$ is Euler's constant.*

**Proof.** We first write the sum as usual

$$\sum_{n\le x} d(n) = \sum_{n\le x}\sum_{d\mid n} 1 = \sum_{dk\le x} 1.$$

Then we use Dirichlet's hyperbola method with $y=\sqrt{x}$ (the choice of $y$ will be explained later). We obtain

$$\begin{aligned}
\sum_{dk\le x} 1 &= \sum_{d\le\sqrt{x}}\sum_{k\le\frac{x}{d}} 1 + \sum_{k\le\sqrt{x}}\sum_{d\le\frac{x}{k}} 1 - \sum_{d\le\sqrt{x}}\sum_{k\le\sqrt{x}} 1 \\
&= 2\sum_{d\le\sqrt{x}}\left\lfloor\frac{x}{d}\right\rfloor - \left\lfloor\sqrt{x}\right\rfloor^2 \\
&= 2\sum_{d\le\sqrt{x}}\left(\frac{x}{d} + O(1)\right) - (\sqrt{x} + O(1))^2 \\
&= \left(2x\sum_{d\le\sqrt{x}}\frac{1}{d}\right) - x + O(\sqrt{x}) \\
&= 2x\left(\log\sqrt{x} + \gamma + O\left(\frac{1}{\sqrt{x}}\right)\right) - x + O(\sqrt{x}) \\
&= x\log x + (2\gamma - 1)x + O(\sqrt{x}).
\end{aligned}$$

This completes the proof. □

Here is the reason for choosing $y = \sqrt{x}$ in the above proof.

Let $y \in [1, x]$ be a parameter to be determined. Then we use the hyperbola method to obtain

$$\begin{aligned}
\sum_{dk\le x} 1 &= \sum_{d\le y}\sum_{k\le\frac{x}{d}} 1 + \sum_{k\le\frac{x}{y}}\sum_{d\le\frac{x}{k}} 1 - \sum_{k\le\frac{x}{y}}\sum_{d\le y} 1 \\
&= \sum_{d\le y}\left\lfloor\frac{x}{d}\right\rfloor + \sum_{k\le\frac{x}{y}}\left\lfloor\frac{x}{k}\right\rfloor - \left\lfloor\frac{x}{y}\right\rfloor\lfloor y\rfloor \\
&= \sum_{d\le y}\left(\frac{x}{d} + O(1)\right) + \sum_{k\le\frac{x}{y}}\left(\frac{x}{k} + O(1)\right) - \left(\frac{x}{y} + O(1)\right)(y + O(1)) \\
&= x\sum_{d\le y}\frac{1}{d} + x\sum_{k\le\frac{x}{y}}\frac{1}{k} - x + O\left(y + \frac{x}{y}\right) \\
&= x(\log y + \gamma) + x\left(\log\frac{x}{y} + \gamma\right) - x + O\left(y + \frac{x}{y}\right) \\
&= x\log x + (2\gamma - 1)x + O\left(y + \frac{x}{y}\right).
\end{aligned}$$

We would like to choose $y$ so that the error term $y+\frac{x}{y}$ is minimal. If $y$ is large, then $\frac{x}{y}$ is small but $y$ is large. If $y$ is small, then $\frac{x}{y}$ is large. So the optimal choice is to choose $y$ so that $y=\frac{x}{y}$. That is $y=\sqrt{x}$. Alternatively, we fix $x\geq 1$ and let $g:[1,x]\to\mathbb{R}$ be given by $g(y)=y+\frac{x}{y}$. By using calculus, it is easy to check that $g$ has an absolute minimum at $y=\sqrt{x}$. Therefore we choose $y=\sqrt{x}$ in the proof of Theorem 5.11.

## 5.4. Extremal Orders

While an average order of an arithmetic function gives an idea of its overall behavior, an extremal order gives bounds for its individual values. In this section, we give the extremal orders of $d(n)$, $\omega(n)$, $\Omega(n)$, and $\varphi(n)$. Chebyshev's estimate $\theta(x)\asymp x$ to be proved in the next chapter may be needed. The reader can either assume $\theta(x)\asymp x$ for now or skip this section and come back later after reading the proof of Chebyshev's estimate.

It is an exercise to show that $d(n)\leq 2\sqrt{n}$ for all $n\in\mathbb{N}$ (see Exercise 5.6.20). With a more careful calculation, one can obtain a bit stronger inequality $d(n)\leq\sqrt{3n}$ and $d(n)\leq 8\sqrt[3]{3n/35}$ for all $n\in\mathbb{N}$ (see Exercise 5.6.21). In general, for each $\varepsilon>0$, there exists a constant $c>0$ such that $d(n)\leq cn^{\varepsilon}$ for all $n\in\mathbb{N}$ as shown in the following theorem.

**Theorem 5.12.** *For each $\varepsilon>0$, we have $d(n)\ll n^{\varepsilon}$, and the implied constant depends at most on $\varepsilon$.*

**Proof.** Let $\varepsilon>0$. We write $d(n)/n^{\varepsilon}$ as

$$\begin{aligned}(5.7)\qquad \prod_{p^a\|n}\left(\frac{a+1}{p^{a\varepsilon}}\right)&=\prod_{\substack{p^a\|n\\ p^{\varepsilon}<2}}\left(\frac{a+1}{p^{a\varepsilon}}\right)\prod_{\substack{p^a\|n\\ p^{\varepsilon}\geq 2}}\left(\frac{a+1}{p^{a\varepsilon}}\right)\\ &\leq\prod_{\substack{p^a\|n\\ p^{\varepsilon}<2}}\left(\frac{a+1}{p^{a\varepsilon}}\right)\prod_{\substack{p^a\|n\\ p^{\varepsilon}\geq 2}}\left(\frac{a+1}{2^{a}}\right).\end{aligned}$$

It is well known and can be proved by induction that $2^a\geq a+1$ for every $a\in\mathbb{N}\cup\{0\}$. So the factor on the right-most side of (5.7) is less than or equal to 1. Therefore

$$(5.8)\qquad \frac{d(n)}{n^{\varepsilon}}\leq\prod_{\substack{p^a\|n\\ p^{\varepsilon}<2}}\left(\frac{a+1}{p^{a\varepsilon}}\right).$$

Since the set of primes $p$ satisfying $p^{\varepsilon} < 2$ is finite, we only need to find an upper bound for the function $f : [0, \infty) \to \mathbb{R}$ defined by

$$f(x) = \frac{x+1}{p^{x\varepsilon}}.$$

We see that $f'(x) > 0$ if and only if $x < \frac{1}{\varepsilon \log p} - 1$. Here $\frac{1}{\varepsilon \log p} - 1 > 0$ since we consider the primes $p$ such that $p^{\varepsilon} < 2$. So $f$ is increasing on $\left[0, \frac{1}{\varepsilon \log p} - 1\right]$ and decreasing on $\left[\frac{1}{\varepsilon \log p} - 1, \infty\right)$. Then

$$\frac{x+1}{p^{x\varepsilon}} = f(x) \leq f\left(\frac{1}{\varepsilon \log p} - 1\right) = \frac{p^{\varepsilon}}{e\varepsilon \log p} \text{ for all } x \geq 0.$$

In particular, $p^{\varepsilon}/e\varepsilon \log p > f(0) = 1$. From this and (5.8), we obtain

$$\frac{d(n)}{n^{\varepsilon}} \leq \prod_{\substack{p^a \| n \\ p < 2^{\frac{1}{\varepsilon}}}} \left(\frac{p^{\varepsilon}}{e\varepsilon \log p}\right) \leq \prod_{p < 2^{\frac{1}{\varepsilon}}} \left(\frac{p^{\varepsilon}}{e\varepsilon \log p}\right) = c,$$

where $c$ is a constant depending only on $\varepsilon$. This completes the proof. □

In most applications, the bound given in Theorem 5.12 is good enough. By using Chebyshev's estimate, we can obtain the maximal order of $\log d(n)$ which shows that the bound $d(n) \ll n^{\varepsilon}$ is not far from being optimal:

$$d(n) \ll n^{\frac{(1+\varepsilon)(\log 2)}{\log \log n}}.$$

Since maximal and minimal orders involve the limit supremum and limit infimum, let us recall their definitions as follows.

**Definition 5.13.** Let $(x_n)$ be a sequence of real numbers. The *limit supremum* of $(x_n)$, denoted by $\limsup_{n\to\infty} x_n$, is defined by

$$\limsup x_n = \lim_{n\to\infty} \left(\sup\{x_k \mid k \geq n\}\right).$$

The *limit infimum* of $(x_n)$, denoted by $\liminf_{n\to\infty} x_n$, is defined by

$$\liminf x_n = \lim_{n\to\infty} \left(\inf\{x_k \mid k \geq n\}\right).$$

It is well known that $\limsup x_n$ and $\liminf x_n$ always exist in the extended real numbers system $\mathbb{R} \cup \{+\infty, -\infty\}$ and they have a property similar to supremum, infimum, and the ordinary limit as shown in the following theorem.

**Theorem 5.14.** *Let $\ell \in \mathbb{R}$ and let $(x_n)$ be a sequence of real numbers. Then*

(i) $\limsup x_n = \ell$ *if and only if* (*a*) *for every* $\varepsilon > 0$*, there exists* $N \in \mathbb{N}$ *such that* $x_n < \ell + \varepsilon$ *for all* $n \geq N$*, and* (*b*) *for every* $\varepsilon > 0$*,* $x_n > \ell - \varepsilon$ *for infinitely many* $n \in \mathbb{N}$*.*

(ii) $\liminf x_n = \ell$ *if and only if* (*a*) *for every* $\varepsilon > 0$*, there exists* $N \in \mathbb{N}$ *such that* $x_n > \ell - \varepsilon$ *for all* $n \geq N$*, and* (*b*) *for every* $\varepsilon > 0$*,* $x_n < \ell + \varepsilon$ *for infinitely many* $n \in \mathbb{N}$*.*

**Remark 5.15.** We can also state Theorem 5.14 without the use of $\varepsilon$ as follows: $\limsup x_n = \ell$ if and only if (a) for every $y > \ell$, there exists $N \in \mathbb{N}$ such that $x_n < y$ for all $n \geq N$ and (b) for every $y < \ell$, $x_n > y$ for infinitely many $n \in \mathbb{N}$. The corresponding statement for $\liminf x_n$ is similar.

**Theorem 5.16.** *The maximal order of* $\log d(n)$ *is* $\frac{(\log 2)(\log n)}{\log\log n}$*. More precisely, we have*

(i) *for* $n \geq 27$*,*

$$\log d(n) \leq \frac{(\log 2)(\log n)}{\log\log n}\left(1 + O\left(\frac{\log\log\log n}{\log\log n}\right)\right),$$

(ii) *if* $n$ *is of the form* $n = \prod_{p \leq x} p$*, then*

$$\log d(n) \geq \frac{(\log 2)(\log n)}{\log\log n}\left(1 + O\left(\frac{1}{\log\log n}\right)\right).$$

**Proof.** Let $n$ be a large positive integer and let $t \in [2, n]$ be a parameter to be determined later. Recall that $k + 1 \leq 2^k$ for all $k \geq 1$. Then

$$d(n) = \prod_{p^k \| n} (k+1) \leq \prod_{p^k \| n,\ p \leq t} (k+1) \prod_{p^k \| n,\ p > t} 2^k.$$

If $p^k \| n$, then $k \leq \frac{\log n}{\log p} \leq \frac{\log n}{\log 2}$, so the first product above is less than or equal to $\left(1 + \frac{\log n}{\log 2}\right)^t$. If $p > t$, then $\log p > \log t$ and

$$2^k \leq 2^{k\frac{\log p}{\log t}} = p^{k\frac{\log 2}{\log t}},$$

so the second product is less than or equal to

$$\left(\prod_{p^k \| n} p^k\right)^{\frac{\log 2}{\log t}} \leq n^{\frac{\log 2}{\log t}}.$$

Therefore $d(n) \le \left(1+\frac{\log n}{\log 2}\right)^t n^{\frac{\log 2}{\log t}}$, and so

$$\log d(n) \le t\log\left(1+\frac{\log n}{\log 2}\right)+\frac{\log 2}{\log t}\log n,$$

since $\log(c+x) \le \log c + \log x$ when $c > 1$ is a constant and $x \to \infty$. So as $n \to \infty$, we have

$$\begin{aligned}\log\left(1+\frac{\log n}{\log 2}\right) &= \log(\log 2 + \log n) - \log\log 2\\ &\le \log(2+\log n) - \log\log 2\\ &\le \log 2 + \log\log n - \log\log 2\\ &\le 2 + \log\log n.\end{aligned}$$

Then

$$\log d(n) \le t(2+\log\log n) + \frac{(\log 2)\log n}{\log t}. \tag{5.9}$$

Recall that if $x \to 0$, then

$$(1-x)^{-1} = 1 + x + x^2 + \cdots = 1 + x(1+x+x^2+\cdots) = 1 + O(x).$$

By choosing $t = \frac{\log n}{(\log\log n)^3}$, we obtain

$$\log d(n) \le \frac{(\log 2)\log n}{\log\log n}\left(1 + O\left(\frac{\log\log\log n}{\log\log n}\right)\right).$$

This proves (i). For (ii), we need an estimate for the function $\theta(x)$ defined by $\theta(x) = \sum_{p\le x}\log p$, which will be proved in Chapter 6. For now, assume that there is a constant $A$ such that $\theta(x) \ge Ax$ for all $x \ge 2$. For each $k \ge 1$, let $n_k = \prod_{i=1}^k p_i$ where $p_i$ is the $i$th prime number. Then

$$d(n_k) = 2^k \text{ and } \log n_k = \sum_{p\le p_k}\log p \le \sum_{p\le p_k}\log p_k = k\log p_k.$$

Therefore

$$\log d(n_k) = k\log 2 \ge \frac{(\log 2)\log n_k}{\log p_k}.$$

Since $\log n_k = \theta(p_k) \ge Ap_k$, we obtain $\log p_k \le \log\log n_k - \log A$. Thus

$$\begin{aligned}\log d(n_k) &\ge \frac{(\log 2)\log n_k}{\log\log n_k - \log A} = \frac{(\log 2)\log n_k}{\log\log n_k}\left(\frac{1}{1+O\left(\frac{1}{\log\log n_k}\right)}\right)\\ &= \frac{(\log 2)\log n_k}{\log\log n_k}\left(1+O\left(\frac{1}{\log\log n_k}\right)\right),\end{aligned}$$

which gives (ii). To prove that $\frac{(\log 2)(\log n)}{\log\log n}$ is the maximal order of $\log d(n)$, we need to show that if $\varepsilon > 0$ is given, then

$$\log d(n) < \frac{(1+\varepsilon)(\log 2)(\log n)}{\log\log n} \text{ for all large } n, \text{ and} \tag{5.10}$$

$$\log d(n) > \frac{(1-\varepsilon)(\log 2)(\log n)}{\log\log n} \text{ for infinitely many } n. \tag{5.11}$$

Since (5.10) and (5.11) follow from (i) and (ii), respectively, the proof is complete. ☐

**Remark 5.17.** It is easy to see that the minimal order of $d(n)$ is 2 since $d(n) \geq 2$ for all $n \geq 2$ and $d(n) = 2$ when $n$ is prime. Similarly, the minimal orders of $\omega(n)$ and $\Omega(n)$ are 1. To determine the maximal orders of $\omega(n)$ and $\Omega(n)$, it is useful to observe the relation given in the next lemma.

**Lemma 5.18.** $2^{\omega(n)} \leq d(n) \leq 2^{\Omega(n)} \leq n$ *for all* $n \in \mathbb{N}$. *The first two inequalities become equalities if and only if* $n$ *is squarefree. In addition,* $2^{\Omega(n)} = n$ *whenever* $n$ *is a power of* 2.

**Proof.** Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $a_1, a_2, \ldots, a_k$ are positive integers. Then

$$d(n) = (a_1+1)(a_2+1)\cdots(a_k+1) \geq (2)(2)\cdots(2) = 2^k = 2^{\omega(n)},$$

and the above is equality if and only if $a_i = 1$ for all $i$, that is, $n$ is squarefree. Since $m + 1 \leq 2^m$ for every $m \in \mathbb{N}$ and $m + 1 = 2^m$ if and only if $m = 1$, we see that $d(n) \leq 2^{a_1} 2^{a_2} \cdots 2^{a_k} = 2^{\Omega(n)}$ with equality if and only if $n$ is squarefree. Finally,

$$2^{\Omega(n)} = 2^{a_1} 2^{a_2} \cdots 2^{a_k} \leq p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = n$$

and this is an equality if $n$ is a power of 2. This completes the proof. ☐

**Theorem 5.19.** *The following statements hold.*

(i) *The maximal order of* $\omega(n)$ *is* $\frac{\log n}{\log\log n}$.

(ii) *The maximal order of* $\Omega(n)$ *is* $\frac{\log n}{\log 2}$.

**Proof.** Let $\varepsilon > 0$. Then by Lemma 5.18 and Theorem 5.16, we obtain

$$\omega(n) \leq \frac{\log d(n)}{\log 2} \leq \frac{(1+\varepsilon)\log n}{\log\log n},$$

for all large $n$. In addition, if $n$ is large and is of the form $n = \prod_{p \le x} p$, then we obtain by Theorem 5.16 and Lemma 5.18 that

$$\omega(n) = \frac{\log d(n)}{\log 2} \ge \frac{(1-\varepsilon)\log n}{\log\log n}.$$

This proves (i). By Lemma 5.18, $\Omega(n) \le \frac{\log n}{\log 2}$ for all $n \in \mathbb{N}$ and this becomes equality for infinitely many $n$. This implies (ii). $\square$

Next we give a result which is useful in solving some exercises.

**Theorem 5.20.** *Let $f$ be a multiplicative function.*

$$\textit{If } \lim_{p^k \to \infty} f(p^k) = 0, \textit{ then } \lim_{n\to\infty} f(n) = 0,$$

*where the first limit is taken over all powers of primes.*

**Proof.** Let $B$ be the set of all prime powers, and assume that $f(q) \to 0$ as $q \in B$ and $q \to \infty$. Then there exists $N_1 \in \mathbb{N}$ such that for every $q \in B \cap [N_1, \infty)$, we have $|f(q)| < 1$. To show that $\lim_{n\to\infty} f(n) = 0$, let $\varepsilon \in (0,1)$ be given. Let

$$M = \max\left\{ \prod_{q\in A} |f(q)| \ : \ A \subseteq B \cap [1, N_1] \right\},$$

where as usual the empty product is defined to be 1. Then $M \ge 1$ and there exists $N_2 \in \mathbb{N}$ such that $N_2 > \max\{N_1+1, M+1\}$ and $|f(q)| < \frac{\varepsilon}{M}$ for every $q \in B \cap [N_2, \infty)$. Let $N$ be the product of all elements in $B \cap [1, N_2]$, and let $n > N$. Then we write $n = \prod_{i=1}^{\infty} p_i^{a_i}$ in the canonical form and group each factor according to its size: $p_i^{a_i} \in [1, N_1]$, $p_i^{a_i} \in (N_1, N_2]$, or $p_i^{a_i} \in (N_2, \infty)$. So we can write $n = n_1 n_2 n_3$ where

$$n_1 = \prod_{p^a \le N_1} p^a, \quad n_2 = \prod_{N_1 < p^a \le N_2} p^a, \quad n_3 = \prod_{p^a > N_2} p^a.$$

By the definition of $M$ and $n_1$, we have $|f(n_1)| \le M$, and by the property of $N_1$, we obtain $|f(n_2)| \le 1$. The product defining $n_1$ and $n_2$ may be empty but by the definition of $N$ and the assumption $n > N$, the product defining $n_3$ is not empty. Therefore

$$|f(n)| = |f(n_1)||f(n_2)||f(n_3)| \le M|f(n_3)| \le M\left(\frac{\varepsilon}{M}\right) < \varepsilon.$$

This completes the proof. $\square$

**Corollary 5.21.** *The following statements hold.*

(i) *For every* $\varepsilon > 0$, *there exists* $N \in \mathbb{N}$ *such that* $\varphi(n) \geq n^{1-\varepsilon}$ *for all* $n \geq N$.

(ii) *For every* $\varepsilon > 0$, *there exists* $N \in \mathbb{N}$ *such that* $\sigma(n) \leq n^{1+\varepsilon}$ *for all* $n \geq N$.

**Proof.** These can be obtained, respectively, by applying Theorem 5.20 to the function $f$ defined by

$$f(n) = n^{1-\varepsilon}/\varphi(n) \text{ and } f(n) = \sigma(n)/n^{1+\varepsilon}. \qquad \square$$

It is trivial that $\varphi(n) \leq n$ and the lower bound $\varphi(n) \geq n^{1-\varepsilon}$ for large $n$ is good enough in many applications. We can also improve this by using estimates involving primes as shown in Theorem 5.22. See also Exercise 5.6.23 for the explicit value of $N$ such that $\varphi(n) \geq n^{1-\varepsilon}$ for all $n \geq N$ when $\varepsilon = 1/2, 1/3$, or $1/4$.

**Theorem 5.22.** *The maximal order of* $\varphi(n)$ *is* $n$. *The minimal order of* $\varphi(n)$ *is*

$$\frac{e^{-\gamma}n}{\log\log n}, \text{ where } \gamma \text{ is Euler's constant.}$$

*The lower bound is asymptotically attained when* $n$ *is of the form* $\prod_{p \leq x} p$, *where we have*

$$\varphi(n) = \frac{e^{-\gamma}n}{\log\log n}\left(1 + O\left(\frac{1}{\log\log n}\right)\right). \tag{5.12}$$

**Proof.** Let $\varepsilon > 0$. Then $\varphi(n) \leq (1+\varepsilon)n$ for every $n \in \mathbb{N}$ and $\varphi(p) = p-1 \geq (1-\varepsilon)p$ for infinitely many primes $p$. Therefore $n$ is the maximal order of $\varphi(n)$. Next suppose $n = \prod_{p \leq x} p$. Then by Mertens' theorem (to be proved in the next chapter),

$$\frac{\varphi(n)}{n} = \prod_{p \leq x}\left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right). \tag{5.13}$$

Since $n = \prod_{p \leq x} p$, we obtain $\log n = \sum_{p \leq x} \log p = \theta(x) \asymp x$, which implies $\log\log n = \log x + O(1)$. Then

$$\begin{aligned}\frac{1}{\log x} &= \frac{1}{\log\log n + O(1)} = \frac{1}{\log\log n}\left(\frac{1}{1 + O\left(\frac{1}{\log\log n}\right)}\right)\\ &= \frac{1}{\log\log n}\left(1 + O\left(\frac{1}{\log\log n}\right)\right).\end{aligned}$$

Substituting the above in (5.13), we obtain (5.12). Next we show that

$$\varphi(n) \geq \frac{(1-\varepsilon)e^{-\gamma}n}{\log\log n} \quad \text{for all large } n\text{, and} \tag{5.14}$$

$$\varphi(n) \leq \frac{(1+\varepsilon)e^{-\gamma}n}{\log\log n} \quad \text{for infinitely many } n. \tag{5.15}$$

Since (5.15) follows immediately from (5.12), it remains to prove (5.14). Let $n$ be a large number and let $m$ be the largest number that is less than or equal to $n$ and is of the form $m = \prod_{i=1}^{k} p_i$ where $p_i$ is the $i$th prime number. Then $m \leq n < \prod_{i=1}^{k+1} p_i$ and therefore $\omega(n) < k+1$. If $B$ is any set containing less than $k+1$ primes, then

$$\frac{\varphi(m)}{m} = \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \leq \prod_{p\in B}\left(1-\frac{1}{p}\right).$$

In particular,

$$\frac{\varphi(m)}{m} \leq \prod_{p|n}\left(1-\frac{1}{p}\right) = \frac{\varphi(n)}{n}.$$

By (5.12), we know that if $m$ is large enough, then

$$\frac{\varphi(m)}{m} \geq \frac{e^{-\gamma}}{\log\log m}(1-\varepsilon).$$

If $n$ is large, then $m$ is large and

$$\frac{\varphi(n)}{n} \geq \frac{\varphi(m)}{m} \geq \frac{e^{-\gamma}}{\log\log m}(1-\varepsilon) \geq \frac{e^{-\gamma}}{\log\log n}(1-\varepsilon).$$

This gives (5.14) and the proof of this theorem is complete. □

**Theorem 5.23.** *The minimal order of $\sigma(n)$ is $n$ and the maximal order of $\sigma(n)$ is $e^{\gamma} n \log\log n$. The maximal order is asymptotically attained when $n$ is of the form $n = \left(\prod_{p\leq x} p\right)^{\lfloor \log x \rfloor}$ where we have*

$$\sigma(n) \geq \frac{e^{\gamma} n \log\log n}{\zeta\left(\frac{1}{2}\log\log n\right)}\left(1 + O\left(\frac{\log\log\log n}{\log\log n}\right)\right). \tag{5.16}$$

**Proof.** Since $\sigma(n) \geq n$ and $\sigma(p)/p = 1 + 1/p \to 1$ as $p \to \infty$, we see that $\liminf_{n\to\infty} \sigma(n)/n = 1$. Next, let $n = \left(\prod_{p\leq x} p\right)^{\lfloor \log x \rfloor}$ and $x$ is large.

Then

$$\frac{\sigma(n)}{n} = \prod_{p\le x}\left(1-\frac{1}{p^{\lfloor \log x\rfloor+1}}\right)\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1}. \tag{5.17}$$

Similar to the proof of Theorem 5.22,

$$\begin{aligned}\log n &= \lfloor \log x\rfloor\,\theta(x) = (\log x + O(1))\,(x+o(x))\\ &= x\log x + o(x\log x),\\ \log\log n &= \log(x\log x)+\log(1+o(1)) = \log x + \log\log x + O(1).\end{aligned}$$

Therefore $\log\log n \gg \log x$, and so $\log\log\log n \gg \log\log x$. Then the second product in (5.17) is $e^\gamma \log x + O(1)$ which is

$$= e^\gamma \log\log n + O(\log\log x) = e^\gamma \log\log n + O(\log\log\log n).$$

For the first product, since $\log\log x \ll \log\log\log n$, we can write $\lfloor \log x\rfloor + 1$ as

$$\log\log n - \log\log x + O(1) \ge \frac{\log\log n}{2} \quad \text{when } n \text{ is large.}$$

Therefore the first product is

$$\ge \prod_p\left(1-\frac{1}{p^{\lfloor \log x\rfloor+1}}\right) \ge \prod_p\left(1-p^{-\frac{\log\log n}{2}}\right) = \frac{1}{\zeta\left(\frac{1}{2}\log\log n\right)}.$$

This proves (5.16). For the maximal order of $\sigma(n)$, we let $\delta > 1$ and observe that $\sigma(n)/n$ is equal to

$$\begin{aligned}\prod_{p^a\|n}\left(1+\frac{1}{p}+\cdots+\frac{1}{p^a}\right) &< \prod_{p|n}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)\\ &= \prod_{p|n}\left(1-\frac{1}{p}\right)^{-1} = \frac{n}{\varphi(n)}.\end{aligned}$$

Since $1/\delta < 1$ and the minimal order $\varphi(n)$ is $e^{-\gamma}n/\log\log n$, there exists $N\in\mathbb{N}$ such that $\varphi(n) > e^{-\gamma}n/(\delta\log\log n)$ for all $n\ge N$. Therefore, for all $n\ge N$,

$$\frac{\sigma(n)}{e^\gamma n\log\log n} < \frac{n}{e^\gamma \varphi(n)\log\log n} < \delta.$$

Observing that $\zeta\left(\frac{1}{2}\log\log n\right) \to 1$ as $n\to\infty$, the remaining part follows from (5.16). This completes the proof. □

It is an exercise to show that $\Lambda(n)$ has maximal order $\log n$, and has no minimal order (see Exercise 5.6.27). Since we restrict ourselves to the case of positive function $g$ as in Definition 5.2, we see that $\mu(n)$ has maximal order 1 and has no minimal order, and $e(n)$ has neither maximal nor minimal order. Since $N(n) = n$ and $1(n) = 1$ for all $n \in \mathbb{N}$, their extremal orders are themselves.

## 5.5. Normal Orders

The concept of normal orders began with the work of Hardy and Ramanujan in [**176**] where they proved that almost all natural numbers $n$ have $\log\log n$ prime factors. Then Turán [**415**] gave a simpler proof of Hardy and Ramanujan's result. Erdös and Kac substantially extended Turán's idea leading to a creation of a subject that is now called probabilistic number theory. For a lot more details about this, we refer the reader to Elliot [**110**, **111**] and Tenenbaum [**407**]. In this section, we present Turán's proof [**415**] that $\omega(n)$ has normal order $\log\log n$ (see Definition 5.3). But we need to use Lemma 9.12 and Theorem 9.13 from Chapter 9. So the reader can either assume those results for now or skip this section and come back later. Similarly, $\Omega(n)$ also has normal order $\log\log n$ and the proof is outlined in Exercise 5.6.30. Generally speaking, if $g(n)$ is an average order of $f(n)$, then we may expect that $g(n)$ should be a good candidate for a normal order of $f(n)$. This is true for $f(n) = \omega(n)$ and $\Omega(n)$ but is false when $f(n) = d(n)$ as will be shown in Theorem 5.28.

**Theorem 5.24.** *We have*

(i) $\displaystyle\sum_{n\le x} \omega^2(n) = x(\log\log x)^2 + O(x\log\log x)$,

(ii) $\displaystyle\sum_{n\le x} (\omega(n) - \log\log x)^2 \ll x\log\log x$,

(iii) $\displaystyle\sum_{2\le n\le x} (\omega(n) - \log\log n)^2 \ll x\log\log x$,

(iv) *if* $\delta > 0$ *is given, then*

$$\#\left\{2 \le n \le x \,:\, |\omega(n) - \log\log n| \ge (\log\log n)^{\frac{1}{2}+\delta}\right\} = o(x),$$

(v) $\omega(n)$ *has normal order* $\log\log n$.

**Proof.** For convenience, we let $p$ and $q$ denote primes. Then

$$\sum_{n\le x}\omega^2(n)=\sum_{n\le x}\sum_{p|n}\sum_{q|n}1=\sum_{p,q\le x}\sum_{\substack{n\le x\\ p|n,q|n}}1=\sum_{\substack{p,q\le x\\ p\ne q}}\left\lfloor\frac{x}{pq}\right\rfloor+\sum_{p\le x}\left\lfloor\frac{x}{p}\right\rfloor.$$

By Theorem 5.8, the last sum above is $\sum_{n\le x}\omega(n)\ll x\log\log x$. For the other sum, if $pq>x$, then $\lfloor x/pq\rfloor=0$, so we write $\sum\lfloor x/pq\rfloor$ as

$$\begin{aligned}\sum_{p,q\le x}\left\lfloor\frac{x}{pq}\right\rfloor-\sum_{p\le x}\left\lfloor\frac{x}{p^2}\right\rfloor&=\sum_{pq\le x}\left\lfloor\frac{x}{pq}\right\rfloor+O(x)\\ &=x\sum_{pq\le x}\frac{1}{pq}+O\left(\sum_{pq\le x}1+x\right).\end{aligned}$$

By Lemma 9.12 and Theorem 9.13, we obtain, respectively,

$$\begin{aligned}\sum_{pq\le x}\frac{1}{pq}&=L_2(x)=(\log\log x)^2+O(\log\log x),\\ \sum_{pq\le x}1&=A_2(x)\ll\frac{x\log\log x}{\log x}.\end{aligned}$$

This implies (i). By squaring out the term $(\omega(n)-\log\log x)^2$ and applying (i) and the formula for $\sum_{n\le x}\omega(n)$, we obtain (ii). For (iii), we use the inequality $(a+b)^2\le 2(a^2+b^2)$ to obtain

(5.18)
$$(\omega(n)-\log\log n)^2\le 2(\omega(n)-\log\log x)^2+2(\log\log x-\log\log n)^2.$$

By (ii), it remains to consider the sum of $(\log\log x-\log\log n)^2$. One way to do this is to square out the terms and calculate the sum of each term over $n\le x$. This leads to

$$\sum_{2\le n\le x}(\log\log x-\log\log n)^2\ll\frac{x\log\log x}{\log x}\ll x. \tag{5.19}$$

Alternatively, we observe that, for $\sqrt{x}<n\le x$, we have

$$\log\log x-1<\log\log x-\log 2=\log\log x^{\frac12}<\log\log n\le\log\log x.$$

Therefore $\log\log n = \log\log x + O(1)$ for $\sqrt{x} < n \le x$ and the sum in (5.19) is

$$\sum_{2\le n\le\sqrt{x}} (\log\log x - \log\log n)^2 + \sum_{\sqrt{x}<n\le x} (\log\log x - \log\log n)^2$$
$$\ll \sqrt{x}(\log\log x)^2 + x \ll x.$$

By (5.18), (5.19), and (ii), we obtain (iii). To prove (iv), let $x$ be a large positive real number. Let $A$ be the set of $n \in \mathbb{N}$ satisfying the inequality in question and for each $y > 0$, let $A(y)$ be the number of elements in $A$ that are $\le y$. Then $A(x) \le \sqrt{x} + A(x) - A(\sqrt{x})$ and $A(x) - A(\sqrt{x})$ is

$$\sum_{\substack{\sqrt{x}<n\le x \\ |\omega(n)-\log\log n|\ge(\log\log n)^{\frac{1}{2}+\delta}}} 1 \le \sum_{\sqrt{x}<n\le x} \left(\frac{\omega(n) - \log\log n}{(\log\log n)^{\frac{1}{2}+\delta}}\right)^2$$
$$\ll \frac{\sum_{n\le x}(\omega(n) - \log\log n)^2}{(\log\log x)^{1+2\delta}} = o(x).$$

(v) Let $\varepsilon > 0$. Let $x$ be a large real number so that

$$(\log\log n)^{-\frac{1}{4}} < \varepsilon \text{ for all } n > \sqrt{x}.$$

Then

$$\#\left\{2 \le n \le x : \left|\frac{\omega(n)}{\log\log n} - 1\right| \ge \varepsilon\right\}$$
$$\le \sqrt{x} + \#\left\{\sqrt{x} < n \le x : |\omega(n) - \log\log n| \ge \varepsilon \log\log n\right\}$$
$$\le \sqrt{x} + \#\left\{\sqrt{x} < n \le x : |\omega(n) - \log\log n| \ge (\log\log n)^{\frac{3}{4}}\right\},$$

which is $o(x)$ by (iv). This shows that $\omega(n)$ has normal order $\log\log n$. □

**Theorem 5.25.** $\Omega(n)$ *has normal order* $\log\log n$.

**Proof.** The proof is outlined in Exercise 5.6.30. □

**Theorem 5.26.** $\log d(n)$ *has normal order* $(\log 2)(\log\log n)$.

**Proof.** Let $\varepsilon > 0$. Since $2^{\omega(n)} \le d(n) \le 2^{\Omega(n)}$, we see that, for $n \ge 3$,

$$\frac{\omega(n)}{\log\log n} - 1 \le \frac{\log d(n)}{(\log 2)(\log\log n)} - 1 \le \frac{\Omega(n)}{\log\log n} - 1.$$

This implies that

$$\left|\frac{\log d(n)}{(\log 2)(\log\log n)} - 1\right| \leq \max\left\{\left|\frac{\omega(n)}{\log\log n} - 1\right|, \left|\frac{\Omega(n)}{\log\log n} - 1\right|\right\}. \tag{5.20}$$

If the left-hand side of (5.20) is $\geq \varepsilon$, then the right-hand side of (5.20) is $\geq \varepsilon$, and so at least one of

$$\left|\frac{\omega(n)}{\log\log n - 1}\right| \text{ and } \left|\frac{\Omega(n)}{\log\log n - 1}\right| \geq \varepsilon.$$

This implies that the set

$$D(x) = \left\{3 \leq n \leq x : \left|\frac{\log d(n)}{(\log 2)(\log\log n)} - 1\right| \geq \varepsilon\right\} \tag{5.21}$$

is a subset of $A(x) \cup B(x)$ where $A(x)$ and $B(x)$ are the sets of $n$ in $[3, x]$ such that $|\omega(n)/\log\log n - 1| \geq \varepsilon$ and $|\Omega(n)/\log\log n - 1| \geq \varepsilon$, respectively. By Theorems 5.24 and 5.25, $|A(x)|$ and $|B(x)|$ are $o(x)$. Since $|A(x) \cup B(x)| \leq |A(x)| + |B(x)|$, we see that $|D(x)|$ is also $o(x)$. This completes the proof. □

There is a bit stronger form of Theorem 5.26 as follows.

**Definition 5.27.** Let $f$ and $g$ be arithmetic functions. We say that $f$ and $g$ are equal *almost everywhere* and write $f(n) = g(n)$ a.e. if the set of positive integers $n$ such that $f(n) = g(n)$ has asymptotic density 1, then

$$\lim_{x\to\infty}\left(\frac{1}{x}\#\{n \leq x : f(n) = g(n)\}\right) = 1.$$

**Theorem 5.28.** *$d(n) = (\log n)^{\log 2 + o(1)}$ a.e.*

**Proof.** We previously proved that

$$\#\left\{2 \leq n \leq x : |\omega(n) - \log\log n| \geq (\log\log n)^{\frac{3}{4}}\right\} = o(x).$$

The above also holds when $\omega(n)$ is replaced by $\Omega(n)$ as shown in Exercise 5.6.30. Let $A$ and $B$ be the sets of all $n \in \mathbb{N}$ such that

$$|\omega(n) - \log\log n| \leq (\log\log n)^{\frac{3}{4}}, |\Omega(n) - \log\log n| \leq (\log\log n)^{\frac{3}{4}},$$

respectively. If $n \in A$, then

$$\begin{aligned} 2^{\omega(n)} &= 2^{\log\log n + \omega(n) - \log\log n} = 2^{\log\log n + O\left((\log\log n)^{\frac{3}{4}}\right)} \\ &= 2^{\log\log n(1+o(1))} = (\log n)^{(\log 2)(1+o(1))} = (\log n)^{\log 2 + o(1)}. \end{aligned}$$

Similarly, if $n \in B$, then $2^{\Omega(n)} = (\log n)^{\log 2 + o(1)}$. Therefore if $n$ is in $A \cap B$, then $d(n) = (\log n)^{\log 2 + o(1)}$. Since $A$ and $B$ have asymptotic density 1, we see that

$$\sum_{\substack{n \le x \\ n \in A \cap B}} 1 \ge \lfloor x \rfloor - \sum_{\substack{n \le x \\ n \notin A}} 1 - \sum_{\substack{n \le x \\ n \notin B}} 1 = x + o(x),$$

and thus $A \cap B$ has asymptotic density 1. So the proof is complete. □

Normal orders of additive functions can generally be obtained from the Turán-Kubilius inequality. We state the result without proof and refer the reader to Elliot [**110**, p. 47].

**Theorem 5.29.** (Turán-Kubilius Inequality) *Let $f$ be a complex-valued additive arithmetic function. For each $x > 0$, let*

$$E(x) = \sum_{p^k \le x} \frac{f(p^k)}{p^k}\left(1 - \frac{1}{p}\right) \quad \textit{and} \quad D(x) = \left(\sum_{p^k \le x} \frac{|f(p^k)|^2}{p^k}\right)^{1/2}.$$

*Then $\sum_{n \le x} |f(n) - E(x)|^2 \le 32 D^2(x)$.*

## 5.6. Exercises

5.6.1 Let $\alpha > 0$ and $\alpha \ne 1$. Show that for $x \ge 2$, we have

(i) $\displaystyle\sum_{n \le x} \frac{d(n)}{n} = \frac{1}{2}\log^2 x + 2\gamma \log x + O(1)$, and

(ii) $\displaystyle\sum_{n \le x} \frac{d(n)}{n^\alpha} = \frac{x^{1-\alpha}\log x}{1-\alpha} + \zeta(\alpha)^2 + O\left(x^{1-\alpha}\right)$.

5.6.2 We know that $\sum_{n=1}^\infty \frac{1}{n^2} = \frac{\pi^2}{6}$ but it is probably less well known that $\sum_{n=1}^\infty \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$. The proof of this result in the literature involves the Euler product formula or the concept of infinite product. This exercise is to give a proof without using the infinite product.

(i) Show that $N = \sigma * \mu$.

(ii) Calculate $\sum_{n \le x} (\sigma * \mu)(n)$ in two ways. One way should lead to the estimate $\frac{x^2}{2} + O(x)$. The other way should lead to

$$\frac{1}{2}\left(\sum_{n=1}^\infty \frac{1}{n^2}\right)\left(\sum_{n=1}^\infty \frac{\mu(n)}{n^2}\right) x^2 + O(x(\log x)^2).$$

(iii) Deduce that $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$.

5.6.3 Let $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. Prove the following statements.

(i) If $\alpha > 0$ and $\alpha \neq 1$, then

$$\sum_{n\le x} \sigma_\alpha(n) = \frac{\zeta(\alpha+1)x^{\alpha+1}}{\alpha+1} + O\left(x^\beta\right),$$

where $\beta = \max\{1, \alpha\}$.

(ii) If $\alpha < 0$ and $\beta = \max\{0, 1+\alpha\}$, then for $x \ge 2$,

$$\sum_{n\le x} \sigma_\alpha(n) = \begin{cases} \zeta(1-\alpha)x + O(x^\beta), & \text{if } \alpha \neq -1; \\ \frac{\pi^2 x}{6} + O(\log x), & \text{if } \alpha = -1. \end{cases}$$

5.6.4 Show that $N^\alpha = \sigma_\alpha * \mu$ and generalize the idea in Exercise 5.6.2. Prove that for each $\alpha > 1$,

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^\alpha} = \frac{1}{\zeta(\alpha)}.$$

5.6.5 Prove that, for $x \ge 2$,

(i) $\displaystyle\sum_{n\le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor^2 = \frac{6x^2}{\pi^2} + O(x \log x)$,

(ii) $\displaystyle\sum_{n\le x} \frac{\mu(n)}{n} \left\lfloor \frac{x}{n} \right\rfloor = \frac{6x}{\pi^2} + O(\log x)$.

5.6.6 Let $x \ge 2$. Show that

(i) $\displaystyle\sum_{n\le x} \varphi(n) = \frac{1}{2} \sum_{n\le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor^2 + \frac{1}{2}$,

(ii) $\displaystyle\sum_{n\le x} \frac{\varphi(n)}{n} = \sum_{n\le x} \frac{\mu(n)}{n} \left\lfloor \frac{x}{n} \right\rfloor$.

Deduce that

$$\sum_{n\le x} \varphi(n) = \frac{3x^2}{\pi^2} + O(x \log x), \qquad \sum_{n\le x} \frac{\varphi(n)}{n} = \frac{6x}{\pi^2} + O(\log x).$$

5.6.7 Let $x \ge 2$. Prove the following statements.

(i) $\displaystyle\sum_{n\le x} \frac{\varphi(n)}{n^2} = \frac{6}{\pi^2} \log x + \frac{6\gamma}{\pi^2} - A + O\left(\frac{\log x}{x}\right)$,

where $A = \displaystyle\sum_{n=1}^{\infty} \frac{\mu(n) \log n}{n^2}$.

(ii) If $\alpha > 1$ and $\alpha \neq 2$, then

$$\sum_{n \le x} \frac{\varphi(n)}{n^\alpha} = \frac{6x^{2-\alpha}}{\pi^2(2-\alpha)} + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} + O\left(x^{1-\alpha} \log x\right).$$

(iii) If $\alpha \le 1$, then

$$\sum_{n \le x} \frac{\varphi(n)}{n^\alpha} = \frac{6x^{2-\alpha}}{\pi^2(2-\alpha)} + O\left(x^{1-\alpha} \log x\right).$$

5.6.8 Prove that for all $x \ge 1$, we have

(i) $\sum_{n \le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1$, and

(ii) $\left| \sum_{n \le x} \frac{\mu(n)}{n} \right| \le 1$.

5.6.9 Show that

$$\sum_{n \le x} \left\{ \frac{x}{n} \right\} = (1-\gamma)x + O(\sqrt{x}).$$

5.6.10 Show that for all $x \ge 2$, we have

(i) $\sum_{n \le x} \Lambda(n) \left\lfloor \frac{x}{n} \right\rfloor = x \log x - x + O(\log x)$, and

(ii) $\sum_{p \le x} (\log p) \left\lfloor \frac{x}{p} \right\rfloor = x \log x + O(x)$.

5.6.11 Prove that

$$\sum_{n \le x} \lambda(n) \left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \sqrt{x} \right\rfloor.$$

5.6.12 Prove that

$$\sum_{n \le x} \left\lfloor \sqrt{\frac{x}{n}} \right\rfloor = \sum_{n \le \sqrt{x}} \left\lfloor \frac{x}{n^2} \right\rfloor.$$

5.6.13 In the proof of Theorem 5.23, we show that

$$\frac{\sigma(n)}{n} < \frac{n}{\varphi(n)} \quad \text{for } n \ge 2.$$

In Chapter 8, we will prove that the infinite product

$$\prod_p (1 - p^{-2}),$$

extended over all primes, converges to $6/\pi^2$. Assuming this result, prove that

(i) $\dfrac{\sigma(n)}{n} < \dfrac{n}{\varphi(n)} < \dfrac{\pi^2}{6}\dfrac{\sigma(n)}{n}$ for $n \geq 2$ and

(ii) $\displaystyle\sum_{n\leq x} \frac{n}{\varphi(n)} \asymp x$.

5.6.14 For each $t \geq 1$, let $R(t) = \sum_{n\leq t} \sigma(n) - \pi^2 t^2/12$. Prove the following statements for $x \geq 2$.

(i) $\displaystyle\sum_{n\leq x} \frac{\sigma(n)}{n^2} = \frac{\pi^2}{6}\log x + B_1 + O\left(\frac{\log x}{x}\right)$, where $B_1$ is a constant given by

$$B_1 = \frac{\pi^2}{12} + 2\int_1^\infty \frac{R(t)}{t^3}dt = \frac{\pi^2\gamma}{6} - \sum_{n=1}^{\infty}\frac{\log n}{n^2}.$$

(ii) If $\alpha > 1$ and $\alpha \neq 2$, then

$$\sum_{n\leq x}\frac{\sigma(n)}{n^\alpha} = \frac{\pi^2 x^{2-\alpha}}{6(2-\alpha)} + B_2 + O\left(\frac{\log x}{x^{\alpha-1}}\right),$$

where $B_2$ is a constant given by

$$B_2 = -\frac{\alpha\pi^2}{12(2-\alpha)} + \alpha\int_1^\infty \frac{R(t)}{t^{\alpha+1}}dt = \zeta(\alpha)\zeta(\alpha-1).$$

(iii) If $\alpha \leq 1$, then

$$\sum_{n\leq x}\frac{\sigma(n)}{n^\alpha} = \frac{\pi^2 x^{2-\alpha}}{6(2-\alpha)} + O\left(x^{1-\alpha}\log x\right).$$

5.6.15 Show that for $x \geq 2$,

$$\sum_{n\leq x}\frac{1}{\varphi(n)} \asymp \log x.$$

5.6.16 For each $n \in \mathbb{N}$, let $f(n) = \sum_{d\mid n}(-1)^d$. Show that

$$f(n) = \begin{cases} -d(n), & \text{if } n \text{ is odd;} \\ 0, & \text{if } 2 \parallel n; \\ d\left(\frac{n}{4}\right), & \text{if } 4 \mid n. \end{cases}$$

5.6.17 Let $f$ be the function given in Exercise 5.6.16 and $\theta \in \left(\frac{1}{4}, \frac{1}{2}\right]$. Suppose that uniformly for $x \geq 2$, we have

$$\sum_{n \leq x} d(n) = x(\log x + 2\gamma - 1) + O\left(x^{\theta}\right), \text{ and}$$

$$\sum_{\substack{n \leq x \\ n \equiv 1 \pmod 2}} d(n) = \frac{x}{4}(\log x + 2\gamma - 1) + O\left(x^{\theta}\right).$$

Show that

(i) $\displaystyle\sum_{n \leq x} f(n) = \sum_{d \leq x} (-1)^d \left\lfloor \frac{x}{d} \right\rfloor = -\left(\frac{\log 2}{2}\right) x + O(x^{\theta})$,

(ii) $\displaystyle\sum_{d \leq x} (-1)^d \left\{\frac{x}{d}\right\} = -\left(\frac{\log 2}{2}\right) x + O\left(x^{\theta}\right)$,

(iii) $\displaystyle\sum_{\substack{n \leq x \\ n \equiv 1 \pmod 2}} \left\{\frac{x}{n}\right\} = \frac{1}{2}\left(1 - \gamma + \frac{\log 2}{2}\right) x + O\left(x^{\theta}\right)$,

(iv) $\displaystyle\sum_{\substack{n \leq x \\ n \equiv 0 \pmod 2}} \left\{\frac{x}{n}\right\} = \frac{1}{2}\left(1 - \gamma - \frac{\log 2}{2}\right) x + O\left(x^{\theta}\right)$.

We note that the coefficients of $x$ on the right-hand sides of (iii) and (iv) are approximately 0.384678 and 0.038105, respectively.

5.6.18 Suppose $f$ is an additive function. Show that

$$\sum_{n \leq x} f(n) = x \sum_{p \leq x} \frac{f(p)}{p} + x \sum_{\substack{p^a \leq x \\ a \geq 2}} \frac{f(p^a) - f(p^{a-1})}{p^a}$$
$$- \sum_{\substack{p^2 \leq x \\ a \geq 1}} \left(f(p^a) - f(p^{a-1})\right) \left\{\frac{x}{p^2}\right\}.$$

Then use the above to prove that

(i) $\displaystyle\sum_{n \leq x} \omega(n) = x \log\log x + bx + O\left(\frac{x}{\log x}\right)$,

(ii) $\displaystyle\sum_{n \leq x} \Omega(n) = x \log\log x + cx + O\left(\frac{x}{\log x}\right)$,

where $b$ and $c$ are constants and $c - b = \sum_p \frac{1}{p(p-1)}$. You may use the fact that $\pi(x) \ll \frac{x}{\log x}$ for $x \geq 2$ and that $\sum_{p \leq x} \frac{1}{p} = \log\log x + b + O\left(\frac{1}{\log x}\right)$, which is proved in the next chapter.

5.6.19 Show that $d(n) \ll n^{\varepsilon}$ for each $\varepsilon > 0$ by applying Theorem 5.20.

5.6.20 Show that $d(n) \le 2\sqrt{n}$ for all $n \in \mathbb{N}$.

5.6.21 Prove the following statements.

(i) $d(n) \le \sqrt{3n}$ for all $n \in \mathbb{N}$ and the equality occurs if and only if $n = 12$.

(ii) $d(n) \le 8\sqrt[3]{3n/35}$ for all $n \in \mathbb{N}$ and the equality occurs if and only if $n = 2520$.

(iii) $d(n) \le 96\sqrt[4]{3n/50050}$ for all $n \in \mathbb{N}$ and the equality occurs if and only if $n = 21621600$.

5.6.22 Let $\varepsilon > 0$, $n \in \mathbb{N}$, and let $N$ be the number of prime factors of $n$ larger than $n^\varepsilon$. Show that $N \le \frac{1}{\varepsilon}$. Deduce that

$$\prod_{p|n}\left(1-\frac{1}{p}\right) \ge 2^{-1/\varepsilon} \prod_{2\le r\le n^\varepsilon}\left(1-\frac{1}{r}\right).$$

Prove that $2^{-1/\varepsilon} n^{1-\varepsilon} \le \phi(n) \le n$.

5.6.23 This exercise is to obtain various lower bounds of $\varphi(n)$.

(i) Show that $\varphi(6) < \sqrt{6}$ and $\varphi(n) \ge \sqrt{n}$ for all $n > 6$.

(ii) Show that the minimum $\left\{\frac{\varphi(n)}{\sqrt{n}} \mid n \in \mathbb{N}\right\}$ exists. What is its value?

(iii) Show that $\varphi(30) < 30^{\frac{2}{3}}$ and $\varphi(n) > n^{\frac{2}{3}}$ for all $n > 30$.

(iv) Show that $\varphi(210) < (210)^{\frac{3}{4}}$ and $\varphi(n) \ge n^{\frac{3}{4}}$ for all $n > 210$. In general, we know that for each $\varepsilon > 0$, there exists $N_\varepsilon \in \mathbb{N}$ such that $\varphi(n) > n^{1-\varepsilon}$ for all $n \ge N_\varepsilon$. What are the values of the smallest such $N_\varepsilon$ for each $\varepsilon = 1/5, 1/6, 1/7$?

(v) Show that $\varphi(n) \ge \pi(n) - \omega(n)$ for all $n \ge 1$ and $\varphi(n) \ge \pi(n)$ for all $n \ge 40$. Find the smallest positive integer $N$ such that $\varphi(n) > \pi(n)$ for all $n \ge N$.

5.6.24 This exercise is to obtain various upper bounds of $\varphi(n)$.

(i) Show that $\varphi(n) < n$ for all $n \ge 2$ and that $\varphi(n) = n - 1$ if and only if $n$ is prime. It is an open problem to prove or disprove that $\varphi(n) \mid n - 1$ implies $n$ is prime.

(ii) Show that if $n - 1 \mid \varphi(n)$, then $n$ is prime.

(iii) Show that $\varphi(n) \le n - \sqrt{n}$ if $n$ is composite.

5.6.25 Recall that $\log n/\log\log n$ is the maximal order of $\omega(n)$. This exercise is to give an upper bound for $\omega(n)$ with an explicit constant. Prove the following statements.

(i) Let $y$ be any real number with $y > 1$. By considering the prime divisors $p$ of $n$ with $p > y$, or otherwise, show that $y^{\omega(n)-y} \le n$, that is, $\omega(n) \le y + \frac{\log n}{\log y}$.

(ii) Show that $f(x) = 2x^{\frac{1}{2}} - \log x$ is an increasing function of $x$ for $x \ge 1$. Deduce that if $n \ge 3$, then

$$(\log n)^{\frac{1}{2}} < \frac{2\log n}{\log\log n}.$$

(iii) Prove that if $n \ge 3$, then

$$\omega(n) \le \frac{4\log n}{\log\log n}.$$

5.6.26 Show that $\lim_{n\to\infty} \varphi(n) = +\infty$. Find the limit

$$\liminf_{n\to\infty} \frac{\varphi(n)\log\log n}{n}.$$

5.6.27 Show that $\log n$ is the maximal order of $\Lambda(n)$. Show also that $\liminf_{n\to\infty} \Lambda(n) = 0$ and $\Lambda(n)$ has no minimal order.

5.6.28 Let $f$ and $g$ be arithmetic functions such that $f = g*1$. Suppose that $\sum_{n=1}^{\infty} \frac{g(n)}{n}$ converges absolutely. Show that

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} f(n) = \sum_{n=1}^{\infty} \frac{g(n)}{n}.$$

5.6.29 Let $Q(x)$ be the number of squarefree positive integers less than or equal to $x$. Show that

$$Q(x) = \frac{6}{\pi^2}x + O(\sqrt{x}).$$

In general, show that if $Q_k(x)$ is the number of $k$th power free integers less than or equal to $x$, then

$$Q_k(x) = \frac{x}{\zeta(k)} + O\left(x^{1/k}\right), \quad \text{where } \zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}.$$

5.6.30 Prove the following statements and show that the normal order $\Omega(n)$ is $\log\log n$. You can use the results which are proved in the next chapter.

(i) $\sum_{n\le x} \Omega^2(n) = x(\log\log x)^2 + O(x\log\log x)$.

(ii) $\sum_{n\le x} (\Omega(n) - \log\log x)^2 \ll x\log\log x$.

(iii) $\sum_{2\le n\le x} (\Omega(n) - \log\log n)^2 \ll x \log\log x.$

(iv) If $\delta > 0$ is given, then

$$\#\left\{2 \le n \le x : |\Omega(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\delta}\right\} = o(x).$$

(v) $\Omega(n)$ has normal order $\log\log n$.

5.6.31 Let $\alpha > 1$. Show that the minimal order of $\sigma_\alpha(n)$ is $n^\alpha$ and a maximal order of $\sigma_\alpha(n)$ is $\zeta(\alpha)n^\alpha$.

5.6.32 Recall that $\log d(n)$ has normal order $(\log 2)(\log\log n)$. Show that $\log\varphi(n)$ has normal order $\log n$. If $k \ge 1$, prove that $\log\sigma_k(n)$ has normal order $k\log n$.

## 5.7. Notes

We first summarize the average orders, extremal orders, and normal orders of some arithmetic functions we have studied. We give the proofs for most of those given below but there are some exceptions. The exceptional case is either trivial or highly nontrivial. For example, the average orders of $d(n)$, $\varphi(n)$, $\sigma(n)$, $\omega(n)$, and $\Omega(n)$ are proved in Section 5.2. Those of $N(n)$, $1(n)$, and $e(n)$ are easy and are left as exercises. The estimate $\sum_{n\le x}\Lambda(n) \sim x$ is much more difficult and will be given in Chapter 9. The $**$ at the maximal order of $d(n)$ in the table indicates that this is not an accurate answer since we only obtain the maximal order for $\log d(n)$ but not for $d(n)$. The $o(1)$ term there only means that

$$d(n) \le n^{\frac{(1+\varepsilon)\log 2}{\log\log n}} \text{ for } n \text{ large and} \tag{5.22}$$

$$d(n) \ge n^{\frac{(1-\varepsilon)\log 2}{\log\log n}} \text{ for infinitely many } n, \tag{5.23}$$

and a better estimate is given in the work of Ramanujan ([**336**], [**339**, pp. 78–128]). For example, Ramanujan showed that $\varepsilon$ in (5.22) and (5.23) can be replaced by $O\left((\log\log n)^{-1}\right)$. We recommend the interested reader to find more details in [**339**], and also in some of the subsequent articles and extensions by other mathematicians [**71**, **113**, **118**, **301**].

Since we require a normal order to be a positive and monotone function, $\Lambda(n)$ has no normal order. But $\Lambda(n) = 0$ for almost all $n$ in $\mathbb{N}$, so we write $\Lambda(n) = 0$ a.e. in the table. Similarly, we proved that $\log d(n)$ has normal order $(\log 2)(\log\log n)$ and $d(n) = (\log n)^{\log 2+o(1)}$ a.e. but these do not imply that $(\log n)^{\log 2}$ is a normal order of $d(n)$. Therefore we put $*$ in the column of normal order of $d(n)$ to mean that it is not actually a normal order. In fact, $d(n)$ has no normal order. Segal [**357**] showed that there does not exist an increasing function $g$ such that $\varphi(n)$ has normal order $g(n)$. Then three years later, Birch [**54**] gave a general criterion implying that $d(n)$, $\varphi(n)$, $\sigma(n)$, and many other popular multiplicative functions have no normal order. The statement of his theorem is given below. See also Klazar's explanation notes [**228**] on the proof of Birch's theorem. The summary of orders is given in the following table.

| | average order | minimal order |
|---|---|---|
| $d(n)$ | $\log n$ | 2 |
| $\varphi(n)$ | $6n/\pi^2$ | $\frac{e^{-\gamma}n}{\log\log n}$ |
| $\sigma(n)$ | $\pi^2 n/6$ | $n$ |
| $\omega(n)$ | $\log\log n$ | 1 |
| $\Omega(n)$ | $\log\log n$ | 1 |
| $\Lambda(n)$ | 1 | does not exist |
| $N(n)$ | $n$ | $n$ |
| $1(n)$ | 1 | 1 |
| $e(n)$ | $1/2^n$ | does not exist |

| | maximal order | normal order |
|---|---|---|
| $d(n)$ | $**\, n^{\frac{\log 2+o(1)}{\log\log n}}$ | $*(\log n)^{\log 2+o(1)}$ a.e. |
| $\varphi(n)$ | $n$ | does not exist |
| $\sigma(n)$ | $e^{\gamma} n\log\log n$ | does not exist |
| $\omega(n)$ | $\log n/\log\log n$ | $\log\log n$ |
| $\Omega(n)$ | $\log n/\log 2$ | $\log\log n$ |
| $\Lambda(n)$ | $\log n$ | $\Lambda(n)=0$ a.e. |
| $N(n)$ | $n$ | $N(n)=n$ always |
| $1(n)$ | 1 | $1(n)=1$ always |
| $e(n)$ | does not exist | $e(n)=0$ a.e. |

**Theorem 5.30.** (Birch [**54**]) *Let $f:\mathbb{N}\to[0,\infty)$ be a multiplicative function which is unbounded and has an increasing normal order. Then there exists a constant $\alpha>0$ such that $f(n)=n^{\alpha}$ for all $n\in\mathbb{N}$.*

Since $d(n)$, $\varphi(n)$, $\sigma(n)$ do not have normal order, the better question to ask is not about their normal orders, but about the existence or nonexistence of the distribution function. A function $D : \mathbb{R} \to \mathbb{R}$ is called a distribution function if $D$ is increasing ($x \leq y$ implies $D(x) \leq D(y)$), right-continuous, $\lim_{u\to-\infty} D(u) = 0$ and $\lim_{u\to+\infty} D(u) = 1$.

We say that an arithmetic function $f$ has a distribution function if there is a distribution function $D_f$ such that

$$\lim_{x\to\infty} \frac{\#\{n \leq x \mid f(n) \leq u\}}{x} = D_f(u),$$

whenever $u$ is a point of continuity of $D_f$. Davenport showed that $\sigma(n)/n$ has a distribution function. Then Erdös and Winter extended it by giving necessary and sufficient conditions for any real-valued additive functions to have a distribution function. The interested reader can find more explanations about this in the book by Pollack [**299**, Chapter 8] and references therein.

Next, consider the error terms in the estimate for the partial sums $\sum_{n\leq x} \sigma(n)$ and $\sum_{n\leq x} \varphi(n)$. Let

$$\Delta_1(x) = \sum_{n\leq x} \sigma(n) - \frac{\pi^2}{12}x^2 \quad \text{and} \quad \Delta_2(x) = \sum_{n\leq x} \varphi(n) - \frac{3}{\pi^2}x^2.$$

Theorems 5.5 and 5.7 tell us that $\Delta_1(x)$ and $\Delta_2(x)$ are $O(x\log x)$. The best results known to date are due to Walfisz [**431**, p. 99 and p. 144] who showed that

$$\Delta_1(x) \ll x(\log x)^{2/3} \text{ and } \Delta_2(x) \ll x(\log x)^{2/3}(\log\log x)^{4/3}.$$

This was proved in 1963 but so far there is no improvement on this estimate.

In the proof of Theorem 5.7, we consider the sum $\sum_{dk\leq x} k\mu(d)$. We chose to fix $d$ and calculate the sum over $k$ as

$$\sum_{d\leq x} \mu(d) \sum_{k\leq \frac{x}{d}} k$$

to obtain the desired result. In this situation, we cannot calculate the sum over $d$ before $k$ because we do not know a simple asymptotic formula of $\sum_{n\leq x} \mu(n)$. In fact, we do not even have a satisfying upper bound for $\sum_{n\le x}\mu(n)$. For example, it is trivial to show that

$$\left|\sum_{n\le x}\mu(n)\right|\le x.$$

However, we expect that there are some cancellations in the sum and we should get

$$\sum_{n\le x}\mu(n)\ll x^{\frac{1}{2}+\varepsilon} \tag{5.24}$$

for any $\varepsilon>0$. At least we should be able to prove $\sum_{n\le x}\mu(n)\ll x^{1-\delta}$ for some $\delta>0$ but this is still an unsolved problem. A well-known nontrivial bound is [**273**, p. 182]

$$\sum_{n\le x}\mu(n)\ll x\exp(-c\sqrt{\log x}),$$

where $c$ is an absolute constant. A better upper bound for the partial sum of $\mu(n)$ can also be obtained from an improvement of the zero free region too, and it leads to the replacement of $\sqrt{\log x}$ by $(\log x)^{\delta}$ for some $\delta>1/2$. More precisely, we have [**211**, p. 309]

$$\sum_{n\le x}\mu(n)\ll x\exp\Big(-c(\log x)^{\frac{3}{5}}(\log\log x)^{-\frac{1}{5}}\Big).$$

In fact (5.24) is equivalent to the Riemann hypothesis and if you can prove it, you will get 1 million US dollars from the Clay Mathematics Institute.

Next, consider the error term in the approximation of $\sum_{n\le x}d(n)$. Let

$$\Delta(x)=\sum_{n\le x}d(n)-x\log x-(2\gamma-1)x.$$

By Theorem 5.11, we know that $\Delta(x)\ll\sqrt{x}$. A famous unsolved problem known as the Dirichlet divisor problem is the determination of the smallest real number $\alpha$ such that $\Delta(x)\ll x^{\alpha+\varepsilon}$ for any $\varepsilon>0$. Voronoï [**430**] obtained that $\Delta(x)\ll x^{\frac{1}{3}+\varepsilon}$. Hardy [**173**] and Landau [**239**] independently proved that $\Delta(x)$ is not $o(x^{\frac{1}{4}})$. So $1/4\le\alpha\le 1/3$ and it is conjectured that $\alpha=1/4$. Many mathematicians have worked on this problem but it is still unsolved. About 114 years after Voronoï, Bourgain [**59**] published a new result on exponential sums and the Riemann zeta function, and then Bourgain and Watt [**60**] adapted the method in [**59**] to show that $\alpha < 517/1648 \approx 0.31371$, which is the best upper bound for $\alpha$ known to date. We summarize the time-line concerning the improvement on the size of $\Delta(x)$ below. For more information, see for example in [**59**, **60**, **204**, **205**, **213**, **354**, **437**]. In particular, we recommend the reader to read the survey article by Berndt, Kim, and Zaharescu [**50**] for a lot more details on both the Dirichlet divisor problem and the Gauss circle problem.

- Voronoï (1903) $\Delta(x) \ll x^{\frac{1}{3}+\varepsilon}$ (0.33333...)
- Hardy and Landau (1916) $\Delta(x) \ll x^{\theta} \to \theta \geq \frac{1}{4}$
- van der Corput (1922) $\Delta(x) \ll x^{\frac{33}{100}+\varepsilon}$ (0.33)
- van der Corput (1928) $\Delta(x) \ll x^{\frac{27}{82}+\varepsilon}$ (0.32926...)
- Chen (1963) $\Delta(x) \ll x^{\frac{12}{37}}$ (0.32432...)
- Kolesnik (1982) $\Delta(x) \ll x^{\frac{35}{108}}$ (0.32407...)
- Vinogradov (1985) $\Delta(x) \ll x^{\frac{17}{53}}$ (0.32075...)
- Iwaniec and Mozzochi (1988) $\Delta(x) \ll x^{\frac{7}{22}+\varepsilon}$ (0.31818...)
- Huxley (1993) $\Delta(x) \ll x^{\frac{23}{73}+\varepsilon}$ (0.31506...)
- Huxley (2003) $\Delta(x) \ll x^{\frac{131}{416}+\varepsilon}$ (0.31490...)
- Bourgain and Watt (2017) $\Delta(x) \ll x^{\frac{517}{1648}+\varepsilon}$ (0.31371...).

Exercises in this chapter are collected from various sources but we also put in something new. Specifically, the author designed Exercises 5.6.2 and 5.6.4 to give a proof, without involving the Euler product formula or the concept of infinite product, of the fact that

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}} = \frac{1}{\zeta(\alpha)} \quad \text{for all } \alpha > 1.$$

Exercises 5.6.16 and 5.6.17 seem to be new too. Although the formula for the sum $\sum d(n)$ where $n$ ranges over $n \leq x$ and $n \equiv 1 \pmod 2$ is not proved in this book, the reader can find a proof of a more general result in [**327**] where the condition $n \equiv 1 \pmod 2$ is replaced by $n \equiv a \pmod q$ for any $q \geq 2$ and $a \in \mathbb{Z}$. More precisely, Pongsriiam and Vaughan [**327**] proved that

(5.25)

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} d(n) = \frac{x}{q}\sum_{t|q}\frac{c_t(a)}{t}\left(\log\frac{x}{t^2}+2\gamma-1\right)+O\left(x^{\frac{1}{3}+\varepsilon}+q^{\frac{1}{2}+\varepsilon}\right)$$

holds uniformly for $a \in \mathbb{Z}$ and $2 \le q \le x$. By the results of Voronoï [**430**] and (5.25), we can take $\theta = 1/3 + \varepsilon$ in Exercise 5.6.17. It shows particularly that when $x$ is large,

$$\sum_{\substack{n\le x\\ n\equiv 1(\bmod 2)}} \left\{\frac{x}{n}\right\} > \sum_{\substack{n\le x\\ n\equiv 0(\bmod 2)}} \left\{\frac{x}{n}\right\}.$$

In addition, a similar calculation also gives

$$\begin{aligned}\sum_{\substack{n\le x\\ n\equiv 0(\bmod 2)}} \left\lfloor\frac{x}{n}\right\rfloor &= \sum_{n\le x} d^{\text{even}}(n)\\ &= \frac{1}{2}x\log x+\frac{1}{2}\left(2\gamma-1-\frac{\log 2}{2}\right)x+O(\sqrt{x}),\end{aligned}$$

$$\begin{aligned}\sum_{\substack{n\le x\\ n\equiv 1(\bmod 2)}} \left\lfloor\frac{x}{n}\right\rfloor &= \sum_{n\le x} d^{\text{odd}}(n)\\ &= \frac{1}{2}x\log x+\frac{1}{2}\left(2\gamma-1+\frac{\log 2}{2}\right)x+O(\sqrt{x}),\end{aligned}$$

where $d^{\text{even}}(n)$ and $d^{\text{odd}}(n)$ are the number of even and the number of odd positive divisors of $n$. This shows that, on average, the positive integers have more odd divisors than even divisors.

Exercise 5.6.20 is well known and the proof of Theorem 5.12 can be adjusted to obtain a sharp upper bound for

$$\frac{d(n)}{\sqrt{n}},\ \frac{d(n)}{\sqrt[3]{n}},\ \frac{d(n)}{\sqrt[4]{n}},$$

and so on, as shown in Exercise 5.6.21. In general, if $\varepsilon > 0$ is given, then there are $c_\varepsilon > 0$ and $N_\varepsilon \in \mathbb{N}$ such that $d(n) \le c_\varepsilon n^\varepsilon$ for all $n \in \mathbb{N}$ and the equality occurs at $n = N_\varepsilon$. When $\varepsilon = 1/2, 1/3, 1/4$, we show in Exercise 5.6.21 that

$$c_\varepsilon = \sqrt{3}, 8\sqrt[3]{3/35}, 96\sqrt[4]{3/50050} \text{ and } N_\varepsilon = 12, 2520, 21621600,$$

respectively. What are the values of $c_\varepsilon$ and $N_\varepsilon$ for each $\varepsilon = 1/n$? Is there anything interesting about the sequence

$$(N_{1/n})_{n\geq 1} = (1, 12, 2520, 21621600, \ldots)?$$

Exercise 5.6.23 gives analogous results for $\varphi(n)$ and a similar question can be asked: what are the values of $N_\varepsilon$ for each $\varepsilon = 1/n$? When $\varepsilon = 1/2, 1/3, 1/4$, we have

$$N_\varepsilon = 2 \times 3, 2 \times 3 \times 5, 2 \times 3 \times 5 \times 7,$$

respectively. Does $N_{1/n} \sim \prod_{p\leq n} p$? Or does $N_{1/n}/\prod_{p\leq n} p$ tend to a limit?

Exercise 5.6.28 is called Wintner's Theorem [**436**]. Axer replaced the absolute convergence of $\sum_{n=1}^{\infty} g(n)/n$ by the convergence of $\sum_{n=1}^{\infty} g(n)/n$ and the additional assumption that $\sum_{d\leq x} |g(d)| \ll x$; see for instance in [**102**, pp. 84–89]. Delange [**101**] improved it to the following form: if $f$ is a multiplicative function, $|f(n)| \leq 1$ for all $n \in \mathbb{N}$, and $\sum_p \frac{1-f(p)}{p}$ converges, then

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} f(n) = \prod_p \left(1 - \frac{1}{p}\right)\left(1 + \sum_{k=1}^{\infty} \frac{f(p^k)}{p^k}\right).$$

Exercise 5.6.29 is a well-known result. It is possible to obtain the main term in Exercise 5.6.29 quickly by applying Wintner's Theorem and the Euler product formula (to be given in Chapter 8): if $f$ is a characteristic function of the $k$th power free integers, then $f$ is multiplicative and

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_p (1 + p^{-s} + \cdots + p^{-(k-1)s}) = \frac{\zeta(s)}{\zeta(ks)} = \zeta(s)G(s),$$

where $G(s) = 1/\zeta(ks) = \sum_{n=1}^{\infty} g(n)n^{-s}$ where $g$ is an arithmetic function and $\zeta$ is the Riemann zeta function. Then Wintner's theorem implies that $\sum_{n\leq x} f(n) \sim G(1)x = x/\zeta(k)$, as required. Exercise 5.6.9 is taken from Vaughan's lecture and he refers it to de la Vallée Poussin. Exercises 5.6.22 and 5.6.25 also came from Vaughan; see also in Montgomery and Vaughan [**273**, p. 39 and pp. 71–75]. For many other interesting theorems on various arithmetic functions, we recommend the reader to follow the work of Professors Erdös, Ford, Pomerance, Luca, Pollack, Banks, and their coauthors.

Chapter 6

# Elementary Results on the Distribution of Primes

## 6.1. Introduction

For each $x \in \mathbb{R}$, let $\pi(x)$ be the number of primes that are less than or equal to $x$. So, for example, $\pi(1) = 0$, $\pi(3) = 2$, $\pi(10) = 4$, and by Euclid's theorem, $\pi(x) \to \infty$ as $x \to \infty$. At this point, it is natural to ask how fast $\pi(x)$ tends to $\infty$ as $x \to \infty$. Can we find an elementary function $g$ such that $\pi(x)$ is well approximated by $g(x)$ as $x \to \infty$? Gauss and Legendre independently predicted that

$$\pi(x) \sim \frac{x}{\log x} \quad \text{as } x \to \infty.$$

Then about 100 years later, Hadamard and de la Vallée Poussin independently proved in 1896 that Gauss and Legendre's conjecture is true, and the statement $\pi(x) \sim x/\log x$ is now known as the prime number theorem. In fact, Gauss made a conjecture in a different form:

$$\pi(x) \sim \int_2^x \frac{1}{\log t}\,dt.$$

But the logarithmic integral $\int_2^x \frac{1}{\log t}dt$ is asymptotic to $x/\log x$, so these two versions are equivalent. We will give a proof of the prime number theorem in Chapter 9. In this chapter, we present elementary results concerning $\pi(x)$ and related functions, and in particular, a proof of Chebyshev's estimate, which is the first substantial progress toward the prime number theorem.

We remind the reader to what has become a standard notation in number theory that $p$ with or without subscripts always denotes a prime number. The summations or products of the form

$$\sum_{p|n}, \quad \sum_{p\le x}, \quad \sum_{p=2}^{\infty}, \quad \prod_{p|n}, \quad \prod_{p\le x}, \quad \prod_{p=2}^{\infty}$$

are taken over prime numbers. In addition, we let $x$ be a real and positive variable, $\log x$ the natural logarithm of $x$, and $n$ a positive integer. The following functions play a central role in the study of the distribution of prime numbers.

**Definition 6.1.** Define the functions $\pi, \theta, \psi : (0,\infty) \to \mathbb{R}$ by

$$\pi(x) = \sum_{p\le x} 1, \quad \theta(x) = \sum_{p\le x} \log p, \quad \text{and} \quad \psi(x) = \sum_{n\le x} \Lambda(n),$$

where $\Lambda$ is the von Mangoldt function.

Therefore $\pi(x)$ counts the number of primes less than or equal to $x$, $\theta(x)$ counts the number of primes with weight $\log p$ for each prime $p$, and $\psi(x)$ gives each prime power $p^k$ a weight $\log p$. The functions $\theta$ and $\psi$ are called Chebyshev's $\theta$-function, and Chebyshev's $\psi$-function, respectively. We have, for example, $\theta(1) = 0$, $\theta(2) = \log 2$, $\theta(4) = \log 2 + \log 3$, $\psi(1) = 0$, $\psi(4) = \log 2 + \log 3 + \log 2$. It is easy to see from the definition that $\psi(x) \ge \theta(x)$ for every $x \ge 1$, and $\theta(x) \ge \pi(x)$ for every $x \ge 5$. More accurate relations between these functions are given in the following theorems.

**Theorem 6.2.** *For every $x \ge 1$, we have*

$$0 \le \psi(x) - \theta(x) \le \frac{\sqrt{x}(\log x)^2}{2\log 2}. \tag{6.1}$$

*In particular, $\psi(x) = \theta(x) + O\left(\sqrt{x}(\log x)^2\right)$ for $x \ge 2$.*

**Proof.** The first inequality in (6.1) is obvious. For the second one, we write

$$\psi(x) = \sum_{n\le x} \Lambda(n) = \sum_{p^k\le x} \Lambda(p^k) = \sum_{k=1}^{\infty} \sum_{p\le x^{1/k}} \log p = \sum_{k=1}^{\infty} \theta(x^{\frac{1}{k}}).$$

We observe that the sum on $k$ is actually a finite sum since $\theta(x^{\frac{1}{k}}) = 0$ if $x^{\frac{1}{k}} < 2$, or equivalently, $\theta(x^{\frac{1}{k}}) = 0$ for every $k > \frac{\log x}{\log 2}$. Then

$$\psi(x) - \theta(x) = \sum_{2\le k\le \frac{\log x}{\log 2}} \theta(x^{\frac{1}{k}}) \le \theta(\sqrt{x})\frac{\log x}{\log 2}.$$

In addition,

$$\theta(\sqrt{x}) = \sum_{p\le\sqrt{x}} \log p \le \sum_{p\le\sqrt{x}} \log\sqrt{x} \le \sqrt{x}\log\sqrt{x}.$$

Therefore $\psi(x) - \theta(x) \le \frac{\sqrt{x}(\log\sqrt{x})(\log x)}{\log 2}$, which implies the desired result. □

By Chebyshev's estimate which will be proved in the next section, we will see that the error term $O\left(\sqrt{x}(\log x)^2\right)$ in the above theorem can be improved to $O(\sqrt{x})$. See Exercise 6.4.1 for a precise statement.

**Theorem 6.3.** *For $x \ge 2$, we have*

$$\theta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\, dt,$$
$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t(\log t)^2}\, dt.$$

**Proof.** Let $a_n = 1$ if $n$ is a prime number and $a_n = 0$ otherwise. Then $\pi(x) = \sum_{n\le x} a_n$ and

$$\theta(x) = \sum_{p\le x} \log p = \sum_{1<n\le x} a_n \log n = \int_1^x \log t\, d\pi(t)$$
$$= \pi(x)\log x - \int_1^x \frac{\pi(t)}{t}\, dt = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\, dt,$$

where the last equality follows from the fact that $\pi(t) = 0$ if $t < 2$. Alternatively, we can write $\theta(x)$ as

$$\sum_{2 \le n \le x} a_n \log n = \int_{2-}^{x} \log t \, d\pi(t),$$

which leads directly to $\pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\,dt$. Next, let $b_n = \log n$ if $n$ is prime and $b_n = 0$ otherwise. Then $\theta(x) = \sum_{n \le x} b_n$ and $\pi(x)$ is equal to

$$\sum_{2 \le n \le x} \frac{1}{\log n} b_n = \int_{2-}^{x} \frac{1}{\log t}\, d\theta(t) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t(\log t)^2}\, dt.$$

This completes the proof. □

There are actually many statements that are equivalent to the prime number theorem. We give three well-known versions in the next theorem and the other three in the notes.

**Theorem 6.4.** *The following statements are equivalent.*

$$\pi(x) \sim \frac{x}{\log x}. \tag{6.2}$$

$$\theta(x) \sim x. \tag{6.3}$$

$$\psi(x) \sim x. \tag{6.4}$$

**Proof.** By Theorem 6.3, we have

$$\frac{\theta(x)}{x} = \frac{\pi(x)}{x/\log x} - \frac{1}{x}\int_2^x \frac{\pi(t)}{t}\, dt. \tag{6.5}$$

Assume that (6.2) holds. Then $\pi(t) \ll \frac{t}{\log t}$. So

$$\begin{aligned}\frac{1}{x}\int_2^x \frac{\pi(t)}{t}\, dt &\ll \frac{1}{x}\int_2^x \frac{1}{\log t}\, dt = \frac{1}{x}\int_2^{\sqrt{x}} \frac{1}{\log t}\, dt + \frac{1}{x}\int_{\sqrt{x}}^x \frac{1}{\log t}\, dt \\ &\ll \frac{1}{x}\left(\frac{\sqrt{x}}{\log 2}\right) + \frac{1}{x}\left(\frac{x}{\log \sqrt{x}}\right),\end{aligned}$$

which converges to zero as $x \to \infty$. Combining this with (6.5), we see that $\theta(x) \sim x$. So (6.2) implies (6.3). Next, we apply Theorem 6.3 again to obtain

$$\frac{\pi(x)}{x/\log x} = \frac{\theta(x)}{x} + \frac{\log x}{x}\int_2^x \frac{\theta(t)}{t(\log t)^2} dt.$$

Then by assuming (6.3) and using a similar argument, we can show that the second term on the right-hand side of the above equation converges to zero as $x \to \infty$, which implies (6.2). So (6.2) and (6.3) are equivalent. By Theorem 6.2, we see that

$$\lim_{x\to\infty}\left(\frac{\psi(x)}{x} - \frac{\theta(x)}{x}\right) = 0.$$

This implies that (6.3) and (6.4) are equivalent. ☐

## 6.2. Chebyshev's Estimates

Chebyshev was the first to make substantial progress towards Gauss's conjecture that $\pi(x) \sim x/\log x$. In this section, we present a simpler proof of Chebyshev's estimates given by Ramanujan [**337**]. The first proof is slightly modified so that it is less computational and is easy to follow. The second proof follows Ramanujan's computation. The details are as follows.

**Theorem 6.5.** (Chebyshev's estimate) *We have*

$$\psi(x) \asymp x \quad \textit{uniformly for } x \geq 2.$$

*More explicitly, we have*

$$\psi(x) < \frac{3}{2}x \ \textit{ for all } x > 0 \textit{ and } \ \psi(x) > \frac{2}{3}x \ \textit{ for all } x \geq 7.$$

**Proof.** We first observe that if $(a_n)$ is a sequence of nonnegative real numbers decreasing to zero, then $\sum_{n=1}^{\infty}(-1)^{n-1}a_n$ converges and

$$a_1 - a_2 \leq \sum_{n=1}^{\infty}(-1)^{n-1}a_n \leq a_1 - a_2 + a_3.$$

This follows from the alternating series test and by considering the partial sums

$$(a_1 - a_2) + (a_3 - a_4) + (a_5 - a_6) + \cdots \geq a_1 - a_2,$$
$$(a_1 - a_2 + a_3) - (a_4 - a_5) - (a_6 - a_7) - \cdots \leq a_1 - a_2 + a_3.$$

Next, let $T(x) = \sum_{n\leq x} \psi\left(\frac{x}{n}\right)$ for every $x \geq 1$. On one hand,

$$\sum_{n\leq x} \log n = \sum_{n\leq x}\sum_{d|n} \Lambda(d) = \sum_{dk\leq x} \Lambda(d) = \sum_{k\leq x}\sum_{d\leq \frac{x}{k}} \Lambda(d)$$
$$= \sum_{k\leq x} \psi\left(\frac{x}{k}\right) = T(x).$$

On the other hand,

$$\sum_{n\leq x} \log n = \int_1^x \log t\, dt + O(\log x) = x\log x - x + O(\log x).$$

Therefore $T(x) = x\log x - x + O(\log x)$ for $x \geq 2$. Then

$$T(x) - 2T\left(\frac{x}{2}\right) = (\log 2)x + O(\log x) \tag{6.6}$$

for every $x \geq 2$. By the definition of $T(x)$ and the fact that $\psi\left(\frac{x}{2n}\right) = 0$ when $\frac{x}{2} < n \leq x$, we obtain

$$\begin{aligned} T(x) - 2T\left(\frac{x}{2}\right) &= \sum_{n\leq x} \psi\left(\frac{x}{n}\right) - 2\sum_{n\leq \frac{x}{2}} \psi\left(\frac{x}{2n}\right) \\ &= \sum_{n\leq x} \psi\left(\frac{x}{n}\right) - 2\sum_{n\leq x} \psi\left(\frac{x}{2n}\right) \\ &= \sum_{n\leq x} (-1)^{n-1}\psi\left(\frac{x}{n}\right). \end{aligned} \tag{6.7}$$

The last equality in (6.7) is obtained by a direct calculation. In addition, $\psi\left(\frac{x}{n}\right) = 0$ for $n > x$, so the last sum in (6.7) is

$$\sum_{n=1}^{\infty} (-1)^{n-1}\psi\left(\frac{x}{n}\right)$$

and (6.7) becomes

$$T(x) - T\left(\frac{x}{2}\right) = \sum_{n=1}^{\infty} (-1)^{n-1}\psi\left(\frac{x}{n}\right). \tag{6.8}$$

Since the sequence $\left(\psi\left(\frac{x}{n}\right)\right)_{n\geq 1}$ is decreasing to zero, we can apply the observation made earlier to see that

$$\psi(x) - \psi\left(\frac{x}{2}\right) \leq \sum_{n=1}^{\infty} (-1)^{n-1}\psi\left(\frac{x}{n}\right) \leq \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right). \tag{6.9}$$

From (6.6), (6.8), and (6.9), we see that

$$\psi(x)-\psi\left(\frac{x}{2}\right)\le(\log 2)x+O(\log x),\quad\text{and}\tag{6.10}$$

$$\psi(x)-\psi\left(\frac{x}{2}\right)+\psi\left(\frac{x}{3}\right)\ge(\log 2)x+O(\log x).\tag{6.11}$$

Since (6.10) holds for all $x\ge 2$, we have the following inequalities

$$\begin{aligned}\psi(x)-\psi\left(\frac{x}{2}\right)&\le(\log 2)x+O(\log x),\\ \psi\left(\frac{x}{2}\right)-\psi\left(\frac{x}{2^2}\right)&\le\left(\frac{\log 2}{2}\right)x+O(\log x),\\ \psi\left(\frac{x}{2^2}\right)-\psi\left(\frac{x}{2^3}\right)&\le\left(\frac{\log 2}{2^2}\right)x+O(\log x),\\ &\vdots\\ \psi\left(\frac{x}{2^r}\right)-0&\le\left(\frac{\log 2}{2^r}\right)x+O(\log x),\end{aligned}$$

where $r$ is the largest integer such that $2^r<x$. Summing up all the terms above, we obtain

$$\psi(x)\le 2(\log 2)x+O((\log x)^2)\ll x.$$

From (6.11), we have

$$\begin{aligned}\psi(x)&\ge(\log 2)x+\left(\psi\left(\frac{x}{2}\right)-\psi\left(\frac{x}{3}\right)\right)+O(\log x)\\ &\ge(\log 2)x+O(\log x)\gg x.\end{aligned}$$

This completes the proof of the first version. Next, we show the explicit bounds for $\psi(x)$. A few details of the calculations will be left as an exercise to the reader. By Euler's summation formula, we have

$$T(x)=\sum_{n\le x}\log n=x\log x-x+1+a(x)\log x,\tag{6.12}$$

where $-\{x\}\le a(x)\le 1-\{x\}$. This implies that

$$\begin{aligned}T(x)-2T\left(\frac{x}{2}\right)&=x\log 2-1+\left(a(x)-2a\left(\frac{x}{2}\right)\right)\log x+2a\left(\frac{x}{2}\right)\log 2\\ &\le(\log 2)\,x+3\log x+\log 4-1.\end{aligned}\tag{6.13}$$

By a usual technique in calculus, one can show that there exists a large number $N$ such that the above is less than $3x/4$ for all $x\ge N$. With a more careful analysis, we find that we can take $N=320$. Then by (6.8) and (6.9), we have $\psi(x)-\psi(x/2)<3x/4$ for all $x\ge 320$. Then we use a computer to check that $\psi(x)-\psi(x/2)<3x/4$ for $x=1,2,3,\dots,319$. If

$1 \le n \le 319$ and $n < x < n+1$, then $\psi(x) - \psi(x/2) = \psi(n) - \psi(n/2) < 3n/4 < 3x/4$. So we conclude that

$$\psi(x) - \psi(x/2) < 3x/4 \quad \text{for all } x > 0. \tag{6.14}$$

Replacing $x$ by $\frac{x}{2}, \frac{x}{2^2}, \dots, \frac{x}{2^r}$ as in the previous proof, we obtain

$$\psi(x) < 3x/2 \quad \text{for all } x > 0.$$

Similar to (6.13), we have $T(x) - T(x/2) \ge (\log 2)x - 3\log x - 1$ which is larger than $2x/3$ for all $x \ge 800$. Therefore

$$\psi(x) - \psi(x/2) + \psi(x/3) > 2x/3 \quad \text{for all } x \ge 800. \tag{6.15}$$

Thus $\psi(x) > 2x/3$ for all $x \ge 800$. Then we use a computer again to check that $\psi(x) > 2(x+1)/3$ for $x = 7, 8, 9, \dots, 800$ to conclude that $\psi(x) > 2x/3$ for all $x \ge 7$. This completes the proof. ☐

We remark that $\psi(x) > 2x/3$ when $x = 6$ too, but this does not imply that $\psi(x) > 2x/3$ for all $x \ge 6$. If $x \to 7^-$, then

$$\psi(x) = \psi(6) < 2x/3.$$

So 7 is the optimal positive integer for the bound $\psi(x) > 2x/3$. In addition, we can run a computation and obtain (6.15) for $x \ge 27$ but this is not necessary for the proof.

**Corollary 6.6.** *For $x \ge 2$, we have $\theta(x) \asymp x$ and $\pi(x) \asymp \frac{x}{\log x}$.*

**Proof.** This follows from Theorems 6.2, 6.3, and 6.5. The argument applied in the proof of Theorem 6.4 is also useful. The details are left to the reader. ☐

We also give an outline for another way to obtain the inequality $\psi(x) \asymp x$ with explicit constants in Exercise 6.4.10. For the explicit constants in the bounds $\pi(x) \asymp x/\log x$, see Exercise 6.4.11. Explicit upper and lower bounds in the estimates $\theta(x) \asymp x$ are shown in Theorem 6.7 and Exercise 6.4.12. For an update on these kinds of results, see the notes in Section 6.5.

**Theorem 6.7.** *For $x \ge 1$, we obtain $\theta(x) \le (\log 4)x$.*

**Proof.** The crucial point is that $\prod_{n<p\le 2n} p \mid \binom{2n}{n}$. This follows from the fact that for each $p \in (n, 2n]$,

$$p \,\Big|\, \binom{2n}{n}(n!)^2 \quad \text{and} \quad (p, (n!)^2) = 1.$$

Next, by considering the binomial expansion of $(1+1)^{2n}$, we see that $\binom{2n}{n} \leq (1+1)^{2n} = 2^{2n}$. Therefore

$$\prod_{n<p\leq 2n} p \leq 2^{2n} \quad \text{for every } n \geq 1. \tag{6.16}$$

We consider the product $\prod_{p\leq n} p$ and partition the interval $[1, n]$ into subintervals $[1, n/2^r], (n/2^r, n/2^{r-1}], \ldots, (n/2^2, n/2], (n/2, n]$, where $r$ is the largest integer such that $n/2^r \geq 1$. By (6.16), we obtain

$$\begin{aligned}\prod_{p\leq n} p &= \Bigg(\prod_{\frac{n}{2}<p\leq n} p\Bigg)\Bigg(\prod_{\frac{n}{2^2}<p\leq\frac{n}{2}} p\Bigg)\cdots\Bigg(\prod_{p\leq\frac{n}{2^r}} p\Bigg)\\ &\leq 2^{n+\frac{n}{2}+\frac{n}{2^2}+\cdots+\frac{n}{2^r}} \leq 2^{n\left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots\right)} = 4^n.\end{aligned}$$

Therefore $\log\left(\prod_{p\leq n} p\right) \leq \log(4^n)$, which leads to the inequality

$$\theta(n) \leq n\log 4 \quad \text{for all } n \geq 1. \tag{6.17}$$

If $x \in \mathbb{R}$ and $x \geq 1$, then we obtain by (6.17)

$$\theta(x) = \theta(\lfloor x\rfloor) \leq (\log 4)\lfloor x\rfloor \leq (\log 4)x.$$

This completes the proof. □

The previous theorem gives an upper bound for $\theta(x)$. So we next show a lower bound for $\theta(x)$ as follows.

**Theorem 6.8.** $\theta(x) > \frac{x}{12}$ *for all* $x \geq 2$.

**Proof.** We use the estimate from the proof of Theorem 6.5 again. Let $x \geq 800$. Since $\psi(x) = \sum_{k=1}^{\infty}\theta(x^{1/k})$, we obtain

$$\psi(x) - 2\psi(\sqrt{x}) = \sum_{n=1}^{\infty}(-1)^{n-1}\theta\left(x^{\frac{1}{n}}\right).$$

Since $\psi(x) < 3x/2$ and $\psi(x) - 2\psi(\sqrt{x}) \leq \theta(x)$, we have

$$\begin{aligned}\psi(x) - \psi(x/2) + \psi(x/3) &\leq \theta(x) + 2\psi(\sqrt{x}) - \theta(x/2) + \psi(x/3)\\ &\leq \theta(x) - \theta(x/2) + 3\sqrt{x} + x/2.\end{aligned}$$

By (6.15), the left-hand side of the above inequality is larger than $2x/3$, so we obtain

$$\theta(x) - \theta(x/2) > x/6 - 3\sqrt{x} \quad \text{for all } x \geq 800. \tag{6.18}$$

Therefore $\theta(x) > x/6 - 3\sqrt{x} > x/12$ for all $x \geq 1296$. We run a computation on a computer to check that $\theta(x) > (x+1)/12$ for $x = 2, 3, \ldots, 1296$. So we conclude that $\theta(x) > x/12$ for all $x \geq 2$. ☐

**Corollary 6.9.** (Bertrand's Postulate) *For each* $x \geq 1$, *there exists a prime* $p$ *in the interval* $(x, 2x]$.

**Proof.** By (6.18) in Theorem 6.8, we have

$$\theta(x) - \theta(x/2) > x/6 - 3\sqrt{x} > 0 \quad \text{for all } x \geq 800.$$

Therefore

$$\theta(2x) - \theta(x) > 0 \text{ for all } x \geq 400.$$

This implies that there exists a prime $p \in (x, 2x]$ for each $x \geq 400$. Then we straightforwardly check that this is also true when $x \in \mathbb{N}$ and $x < 400$. If $N < p \leq 2N$, then $N + \delta < p \leq 2(N + \delta)$ for every $\delta \in (0, 1)$ and a positive integer $N$. This implies the desired result. ☐

## 6.3. Mertens' Theorems

Certain sums depending on primes $p \leq x$ have an asymptotic behavior which is easier to obtain than that of $\pi(x)$. This is the case for the sum and product given in the next theorem.

**Theorem 6.10.** (Mertens' Theorem) *For* $x \geq 2$, *we have*

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1), \tag{6.19}$$

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1), \tag{6.20}$$

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + b + O\left(\frac{1}{\log x}\right), \tag{6.21}$$

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^c \log x + O(1), \tag{6.22}$$

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-c}}{\log x} + O\left(\frac{1}{(\log x)^2}\right), \tag{6.23}$$

*where* $b$ *in* (6.21) *and* $c$ *in* (6.22) *and* (6.23) *are absolute constants. In fact,* $c = \gamma$ *is the Euler constant.*

**Proof.** By Exercise 6.4.2, we have

$$x\log x - x + O(\log x) = \sum_{d\le x}\Lambda(d)\left\lfloor\frac{x}{d}\right\rfloor,$$

which is also equal to

$$\begin{aligned}\sum_{d\le x}\Lambda(d)\left(\frac{x}{d}+O(1)\right) &= x\sum_{d\le x}\frac{\Lambda(d)}{d}+O(\psi(x))\\ &= x\sum_{d\le x}\frac{\Lambda(d)}{d}+O(x).\end{aligned}$$

So $x\sum_{d\le x}\frac{\Lambda(d)}{d} = x\log x + O(x)$. Dividing both sides by $x$ leads to (6.19). Next, we obtain

$$\sum_{n\le x}\frac{\Lambda(n)}{n} = \sum_{p\le x}\frac{\log p}{p} + \sum_{\substack{p^k\le x\\ k\ge 2}}\frac{\log p}{p^k}, \quad \text{and}$$

$$\begin{aligned}\sum_{\substack{p^k\le x\\ k\ge 2}}\frac{\log p}{p^k} \le \sum_{p\le\sqrt{x}}\sum_{k=2}^{\infty}\frac{\log p}{p^k} &= \sum_{p\le\sqrt{x}}\frac{\log p}{p(p-1)}\\ \le \sum_{n=2}^{\infty}\frac{\log n}{n(n-1)} &\ll 1.\end{aligned}$$

So

$$\sum_{p\le x}\frac{\log p}{p} = \sum_{n\le x}\frac{\Lambda(n)}{n} + O(1) = \log x + O(1),$$

which gives (6.20). Next let $A(x) = \sum_{p\le x}\frac{\log p}{p}$. Then

$$A(x) = \log x + R(x), \quad \text{where } R(x) = O(1).$$

Therefore

$$\begin{aligned}
\sum_{p\le x}\frac{1}{p} &= \sum_{p\le x}\frac{\log p}{p}\frac{1}{\log p} = \int_{2-}^{x}\frac{1}{\log t}\,dA(t)\\
&= \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t(\log t)^2}\,dt\\
&= \frac{\log x + O(1)}{\log x} + \int_2^x \frac{\log t + R(t)}{t(\log t)^2}\,dt\\
&= 1 + \int_2^x \frac{1}{t\log t}\,dt + \int_2^x \frac{R(t)}{t(\log t)^2}\,dt + O\left(\frac{1}{\log x}\right)\\
&= 1 + \log\log x - \log\log 2 + \int_2^\infty \frac{R(t)}{t(\log t)^2}\,dt\\
&\quad - \int_x^\infty \frac{R(t)}{t(\log t)^2}\,dt + O\left(\frac{1}{\log x}\right)\\
&= \log\log x + b - \int_x^\infty \frac{R(t)}{t(\log t)^2}\,dt + O\left(\frac{1}{\log x}\right), \qquad (6.24)
\end{aligned}$$

where $b = 1 - \log\log 2 + \int_2^\infty \frac{R(t)}{t(\log t)^2}\,dt$. Since $R(t) = O(1)$, we see that $\int_2^\infty \frac{R(t)}{t(\log t)^2}\,dt$ converges and

$$\int_x^\infty \frac{R(t)}{t(\log t)^2}\,dt \ll \int_x^\infty \frac{1}{t(\log t)^2}\,dt \ll \frac{1}{\log x}.$$

Combining this with (6.24), we obtain (6.21). Next,

$$\begin{aligned}
\log\left(\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1}\right) &= \sum_{p\le x}\log\left(1-\frac{1}{p}\right)^{-1} = \sum_{p\le x}\sum_{n=1}^{\infty}\frac{1}{np^n}\\
&= \sum_{p\le x}\frac{1}{p} + \sum_{p\le x}\sum_{n=2}^{\infty}\frac{1}{np^n}\\
&= \log\log x + b + \sum_{p}\sum_{n=2}^{\infty}\frac{1}{np^n} - \sum_{p>x}\sum_{n=2}^{\infty}\frac{1}{np^n} + O\left(\frac{1}{\log x}\right). \qquad (6.25)
\end{aligned}$$

Since $\sum_{n=2}^\infty \frac{1}{np^n} \le \sum_{n=2}^\infty \frac{1}{p^n} = \frac{1}{p(p-1)}$, the above series converges and

$$\sum_{p>x}\sum_{n=2}^{\infty}\frac{1}{np^n} \le \sum_{p>x}\frac{1}{p(p-1)} \le \sum_{n>x}\frac{1}{n(n-1)} \ll \frac{1}{x} \ll \frac{1}{\log x}.$$

So (6.25) becomes $\log\log x + c + f(x)$, where $c$ is a constant and $f(x) = O\left(\frac{1}{\log x}\right)$. Then

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} = e^{\log\log x + c + f(x)} = e^c \log x\left(1+\sum_{n=1}^{\infty}\frac{(f(x))^n}{n!}\right),$$

and the sum is $\ll |f(x)| \ll \frac{1}{\log x}$, which gives (6.22). Then the product on the left side of (6.23) is equal to

$$\begin{aligned}\frac{1}{e^c\log x(1+f(x))} &= \frac{e^{-c}}{\log x}\left(1+\sum_{n=1}^{\infty}(-1)^n(f(x))^n\right)\\ &= \frac{e^{-c}}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right).\end{aligned}$$

This proves (6.23). We only need to know that $c$ in (6.22) and (6.23) is a constant. Nevertheless, it can be shown that $c = \gamma$ is the Euler constant. We refer the reader to Montgomery and Vaughan [**273**, Theorem 2.7] for the proof of the equality $c = \gamma$. ☐

## 6.4. Exercises

6.4.1 Show that for $x \ge 2$, we have

$$\begin{aligned}\psi(x) &= \theta(x) + O(\sqrt{x}),\\ \pi(x) &= \frac{\psi(x)}{\log x} + O\left(\frac{x}{(\log x)^2}\right).\end{aligned}$$

6.4.2 Show that for $x \ge 1$,

$$\sum_{d\le x}\Lambda(d)\left\lfloor\frac{x}{d}\right\rfloor = x\log x - x + 1 + R(x),$$

where $-\{x\}\log x \le R(x) \le \log x$.

6.4.3 Show that $\int_1^x \frac{\psi(t)}{t^2}\,dt = \log x + O(1)$.

6.4.4 Show that $\sum_{n\le x}(\Lambda(n))^2 \ll x\log x$.

6.4.5 Prove the following statements by applying the prime number theorem.

(i) If $a > 0$ and $b > 0$, then $\pi(ax)/\pi(bx) \sim a/b$ as $x \to \infty$.

(ii) If $0 < a < b$, there exists an $x_0$ such that $\pi(ax) < \pi(bx)$ if $x \ge x_0$.

- (iii) If $0 < a < b$, there exists an $x_0$ such that for $x \geq x_0$ there is at least one prime in the interval $(ax, bx]$.

6.4.6 If $0 < a < b$, show that the interval $(a, b)$ contains a rational number of the form $p/q$, where $p$ and $q$ are primes. (You can use the result from the previous exercise).

6.4.7 Prove the following statements. (You can use the result from the previous exercise).

- (i) Given a positive integer $n$ there exists a positive integer $k$ and a prime $p$ such that $10^k n < p < 10^k(n+1)$.
- (ii) Given $m$ integers $a_1, \dots, a_m$ such that $0 \leq a_i \leq 9$ for $i = 1, 2, \dots, m$, there exists a prime $p$ whose decimal expansion has $a_1, \dots, a_m$ for its first $m$ digits (counting from the left to the right).

6.4.8 Let $f$ be an arithmetic function such that

$$\sum_{p \leq x} f(p) \log p = (ax + b) \log x + cx + O(1) \quad \text{for } x \geq 2.$$

Prove that there is a constant $A$ (depending on $f$) such that, if $x \geq 2$, then

$$\sum_{p \leq x} f(p) = ax + (a + c)\left(\frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t}\right) + b \log(\log x) + A + O\left(\frac{1}{\log x}\right).$$

6.4.9 Let $A$ be the set of positive integers $n$ that have a prime factor larger than $\sqrt{n}$, and let $A(x)$ be the number of the elements of $A$ that are $\leq x$.

- (i) Show that $A(x) \gg \frac{x}{\log x}$ for $x \geq 2$.
- (ii) Show that $\liminf_{x \to \infty} \frac{A(x)}{x} \geq \log 2$.

6.4.10 This exercise is to give another proof of Chebyshev's estimates $\psi(x) \asymp x$ with explicit constants by following the outline given below.

- (i) Prove that $\operatorname{lcm}[1, 2, 3, \dots, n] = \prod_{p \leq n} p^{\nu(p)}$, where $\nu(p)$ is the largest integer such that $p^{\nu(p)} \leq n$.
- (ii) Prove that $e^{\psi(n)} = \operatorname{lcm}[1, 2, \dots, n]$.
- (iii) Let $I = \int_0^1 x^n (1 - x)^n \, dx$. Show that $0 < I \leq 4^{-n}$.
- (iv) Show that $e^{\psi(2n+1)} I$ is a positive integer.

(v) Prove that $\psi(n) \geq \left(\frac{\log 2}{2}\right) n$ for every $n \geq 2$.

(vi) Prove that $\psi(n) \leq (2 + \log 4)n$ for every $n \geq 2$. Conclude that $x \ll \psi(x) \ll x$ for every $x \geq 2$.

6.4.11 This exercise is to give the estimate $\pi(x) \asymp x/\log x$ with explicit constants.

(i) Prove Legendre's formula

$$v_p(n!) = \sum_{k=1}^{\infty} \lfloor n/p^k \rfloor .$$

(ii) Show that if $n \geq 2$, then $\binom{2n}{n} \mid \prod_{p<2n} p^{r_p}$ where $r_p$ is the largest integer such that $p^{r_p} \leq 2n$.

(iii) Show that $\binom{2n}{n} \leq (2n)^{\pi(2n)}$.

(iv) Show that $2^{2n} < (2n+1)\binom{2n}{n}$.

(v) Show that $2^n < 2^{2n}/(2n+1)$ for all $n \geq 3$.

(vi) Conclude that $\pi(2n) > \left(\frac{\log 2}{2}\right)\left(\frac{2n}{\log 2n}\right)$ for all $n \geq 3$.

(vii) Conclude that $\pi(x) > \frac{3\log 2}{8} \cdot \frac{x}{\log x}$ for all $x \geq 2$.

(viii) Show that $\prod_{n<p\leq 2n} p < 2^{2n}$.

(ix) Show that $\pi(2n)\log n - \pi(n)\log(n/2) \leq (3\log 2)n$.

(x) Conclude that $\pi(x) < \frac{(6\log 2)x}{\log x}$ for all $x \geq 2$.

6.4.12 Show that for $x \geq 10^4$, $\theta(x) \geq \frac{x}{\log 4}$ by following the outline given below.

(i) Let $f(x) = \lfloor x \rfloor - \left\lfloor \frac{x}{2} \right\rfloor - \left\lfloor \frac{x}{3} \right\rfloor - \left\lfloor \frac{x}{5} \right\rfloor + \left\lfloor \frac{x}{30} \right\rfloor$ for all $x \in \mathbb{R}$. Show that $f$ has period 30.

(ii) Show that $f(30 - x) = 1 - f(x)$ for $x \notin \mathbb{Z}$.

(iii) Deduce that $f(x) \in \{0, 1\}$ for all $x \in \mathbb{R}$.

(iv) Conclude that $\psi(x) \geq \sum_{n\leq x} \Lambda(n) f\left(\frac{x}{n}\right)$.

(v) Apply Theorem 6.2 and prove that $\theta(x) \geq x/2$.

6.4.13 Show that for all large $n$, we have

(i) $\sum_{d\mid n} \frac{1}{d} \ll \log\log n$,

(ii) $\sum_{p\mid n} \frac{1}{p} \ll \log\log\log n$.

## 6.5. Notes

As mentioned in the introduction of this chapter, Gauss conjectured that

$$\pi(x) \sim \int_2^x \frac{1}{\log t}\,dt.$$

Although $x/\log x$ and $\int_2^x \frac{1}{\log t}dt$ are asymptotic as $x \to \infty$ and both are good approximations for $\pi(x)$, it turns out that $\int_2^x \frac{1}{\log t}dt$ is a better estimate. In fact, it can be shown that

$$\left|\pi(x) - \frac{x}{\log x}\right| \asymp \frac{x}{(\log x)^2} \quad \text{and}$$

$$\left|\pi(x) - \int_2^x \frac{1}{\log t}dt\right| \ll \frac{x}{(\log x)^A} \quad \text{for any } A > 0.$$

For more details about this, see the prime number theorem given in Chapter 9. An upper bound better than that given in Theorem 6.7 was proved by Hanson [**170**] where he showed that $\theta(x) \le x \log 3$ for $x \ge 2$. The proofs of Theorems 6.5 and 6.8, and Corollary 6.9 are adjusted from those of Ramanujan [**337**]. Exercises 6.4.5 to 6.4.8 are taken from Apostol [**18**, Chapter 4]. Exercise 6.4.10 is from Vaughan's lecture. Exercises 6.4.11 and 6.4.12 are adapted from [**102**, pp. 26–28] and [**58**, p. 83].

Let $p_n$ be the $n$th prime number. It is well known that (6.2), (6.3), and (6.4) given in Theorem 6.4 are also equivalent to each of the following conditions:

$$p_n \sim n\log n, \quad \lim_{x\to\infty}\left(\frac{1}{x}\sum_{n\le x}\mu(n)\right) = 0, \quad \sum_{n=1}^{\infty}\frac{\mu(n)}{n} = 0.$$

We do not need the above result in this text but the interested reader can find a proof of this fact in Apostol [**18**, Theorems 4.5, 4.14, 4.15, 4.16]. Explicit upper and lower bounds of $p_n$ such as

$$\frac{1}{6}n\log n < p_n < 12\left(n\log n + n\log\frac{12}{e}\right)$$

are also given in [**18**, Theorem 4.7].

By sacrificing the range of validity, one can obtain estimates for $\psi(x)$, $\theta(x)$, and $\pi(x)$ in a stronger form than those given in Theorems 6.5, 6.7, and 6.8, and in Exercises 6.4.10 to 6.4.12. With a more careful analysis and computer programming, Rosser and Schoenfeld [**349**] obtained some widely applicable approximations for $\pi(x)$, $\psi(x)$, and $\theta(x)$. We show a few of them below.

$$\begin{aligned}
&\pi(x) > \frac{x}{\log x - \frac{1}{2}} \quad \text{for } x \ge 67,\\
&\pi(x) < \frac{x}{\log x - \frac{3}{2}} \quad \text{for } x > e^{3/2},\\
&\pi(x) > \frac{x}{\log x} \quad \text{for } x \ge 17,\\
&\psi(x) - \theta(x) > 0.98\sqrt{x} \quad \text{for } x \ge 121,\\
&\theta(x) > x\left(1 - \frac{1}{\log x}\right) \quad \text{for } x \ge 41,\\
&\theta(x) < 1.01624x \quad \text{for } x > 0,\\
&\quad p_n > n\left(\log n + \log\log n - \frac{3}{2}\right) \quad \text{for } n \ge 2,\\
&\quad p_n < n\left(\log n + \log\log n - \frac{1}{2}\right) \quad \text{for } n \ge 20.
\end{aligned}$$

Many researchers have improved the above inequalities. We write $f(x) = O^*(g(x))$ to mean $f(x) = O(g(x))$ and the implied constant can be taken to be 1. Dusart [**108**] has recently obtained the following estimates:

$$\begin{aligned}
&\psi(x) = x + O^*(59.2x/(\log x)^4) \quad \text{for } x \ge 2,\\
&\theta(x) = x + O^*(151.3x/(\log x)^4) \quad \text{for } x \ge 2,\\
&\psi(x) - \theta(x) > 0.9999\sqrt{x} \quad \text{for } x \ge 121,\\
&\pi(x) \le \frac{1.2551x}{\log x} \quad \text{for } x > 1,\\
&\pi(x) \ge \frac{x}{\log x - 1} \quad \text{for } x \ge 5393,\\
&\pi(x) \le \frac{x}{\log x - 1.112} \quad \text{for } x > e^{1.112}.
\end{aligned}$$

For more information on results of this kind, we recommend the reader to follow the works of C. Axler, P. Dusart, L. Faber, H. Kadiri, O. Ramaré, G. Robin, B. Rosser, L. Schoenfeld, and their coauthors, to name but a few.

## Chapter 7

# Characters and Dirichlet's Theorem

### 7.1. Introduction

This chapter is devoted to the proof of the famous Dirichlet theorem on primes in arithmetic progressions which states that for every pair of coprime positive integers $a$ and $q$, there are infinitely many primes in the arithmetic progression $a \pmod{q}$. Before Dirichlet, there was an elementary algebraic proof that there are infinitely many primes $p \equiv a \pmod{q}$ if $a$ and $q$ are given explicitly and satisfy certain conditions but there was no proof which works for all $a$ and $q$ with $(a, q) = 1$. In fact, there is currently no nonanalytic proof of Dirichlet's theorem and this result is considered by many mathematicians the birth of analytic number theory.

Our proof of Dirichlet's theorem follows the version given by Shapiro ([**363**], [**364**, Chapter 9]), Apostol [**18**, Chapter 7], Gelfond and Linnik [**142**, Chapter 3], and Pollack [**299**, Chapter 2]. For a shorter proof, we refer the reader to Montgomery and Vaughan [**273**, pp. 121–123]. To understand the material in this chapter, the reader should be familiar with both the calculations in Chapters 4 to 6 and the results in group theory; a background from a course in abstract algebra should be enough.

We first give the basic results on the characters of a finite abelian group in Sections 7.1 and 7.2. Then we introduce the concept of Dirichlet characters and Dirichlet $L$-functions in Sections 7.3 and 7.4. These concepts are actually connected to vast areas of research and we refer the reader to other books and articles for more information. In this book, we only study them to the extent which is enough to give a proof of Dirichlet's theorem in Section 7.5. Examples and exercises concerning characters, an application of Dirichlet's theorem, and other types of integers in an arithmetic progression are given in Sections 7.6 and 7.8. As in the other chapters, the notes on some research problems are given in the last section.

Recall that $\mathbb{C}^\times$, the set of nonzero complex numbers, is a group under the usual multiplication. The definition of a character of a group is as follows.

**Definition 7.1.** A *character* of a group $G$ is a group homomorphism from $G$ into $\mathbb{C}^\times$. In other words, $\chi$ is a character of a group $G$ if $\chi : G \to \mathbb{C}^\times$ satisfying $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in G$. The trivial homomorphism which maps every $g \in G$ to 1 is called the *principal character* of $G$ and is denoted by $\chi_0$.

Next, we define $\widehat{G}$ and the multiplication in it. We will show in Theorem 7.4 that $\widehat{G}$ is a group under this multiplication.

**Definition 7.2.** For each group $G$, we write $\widehat{G}$ to denote the set of all characters of $G$ and we define a multiplication on $\widehat{G}$ by

$$\chi_1\chi_2(g) = \chi_1(g)\chi_2(g) \quad \text{for every } \chi_1, \chi_2 \in \widehat{G} \text{ and } g \in G.$$

Recall that, for each $\theta \in \mathbb{R}$, $e^{i\theta} = \cos\theta + i\sin\theta$ and we write $e(\theta)$ to denote $e^{2\pi i\theta}$. For example, $e(1/n)$ is an $n$th root of unity. A characterization of the characters of a finite cyclic group is as follows.

**Theorem 7.3.** *Assume that $G = \langle g_0 \rangle$ is a cyclic group of order $n$. Then there are exactly $n$ characters $\chi_0, \chi_1, \chi_2, \dots, \chi_{n-1}$ of $G$ given by $\chi_m(g_0^k) = e(mk/n)$ for each $m = 0, 1, \dots, n-1$ and for every $k \in \mathbb{Z}$. That is, $\chi_0(g_0^k) = 1$, $\chi_1(g_0^k) = e(k/n)$, $\chi_2(g_0^k) = e(2k/n)$, …, $\chi_{n-1}(g_0^k) = e((n-1)k/n)$ for every $k \in \mathbb{Z}$.*

**Proof.** Let $\chi$ be a character of $G$. Since $\chi(g_0)^n = \chi(g_0^n) = \chi(1) = 1$, we see that $\chi(g_0)$ is an $n$th root of unity. Therefore $\chi(g_0) = e(m/n)$ for some $m = 0, 1, 2, \ldots, n-1$. Since $G$ is cyclic and is generated by $g_0$, $\chi$ is uniquely determined by $\chi(g_0)$ and $\chi(g_0^k) = (\chi(g_0))^k = e(km/n)$ for every $k \in \mathbb{Z}$. Therefore $\chi = \chi_m$. This shows that if $\chi$ is a character of $G$, then $\chi$ is one of $\chi_0, \chi_1, \ldots, \chi_{n-1}$. Next, we show that $\chi_0, \chi_1, \ldots, \chi_{n-1}$ are well defined and are distinct characters of $G$. If $g_0^{k_1} = g_0^{k_2}$, then $k_1 \equiv k_2 \pmod{n}$ which implies $e\left(\frac{mk_1}{n}\right) = e\left(\frac{mk_2}{n}\right)$ for $0 \le m \le n-1$. Therefore $\chi_0, \chi_1, \ldots, \chi_{n-1}$ are well defined on $G$. If $m_1, m_2 = 0, 1, \ldots, n-1$ and $m_1 \neq m_2$, then

$$\chi_{m_1}(g_0) = e\left(\frac{m_1}{n}\right) \neq e\left(\frac{m_2}{n}\right) = \chi_{m_2}(g_0),$$

which implies that $\chi_0, \chi_1, \ldots, \chi_{n-1}$ are all distinct. It is easy to check that $\chi_0, \chi_1, \ldots, \chi_{n-1}$ are group homomorphisms. Therefore $\chi_0, \chi_1, \ldots, \chi_{n-1}$ are the set of all distinct characters of $G$. $\square$

**Theorem 7.4.** *For every group $G$, the set $\widehat{G}$ is an abelian group under the pointwise multiplication given in Definition* 7.2.

**Proof.** The principal character $\chi_0$ of $G$ is the identity for $\widehat{G}$. If $\chi \in \widehat{G}$ is given, then the function $\chi_1$ given by $\chi_1(g) = 1/\chi(g)$ for every $g \in G$ is the inverse of $\chi$. Other properties can be verified easily. $\square$

**Remark 7.5.** By Theorem 7.4, $\widehat{G}$ is a group and it is called the *dual group* of $G$. The inverse of $\chi$ given in the proof of Theorem 7.4 is usually denoted by $\chi^{-1}$ or $\overline{\chi}$. The reason to write $\chi^{-1}$ is clear. If $\chi$ is a character of a finite abelian group, then $|\chi(g)| = 1$ and $\chi^{-1}(g) = 1/\chi(g) = \overline{\chi(g)}$. Therefore, if we define $\overline{\chi}$ by $\overline{\chi}(g) = \overline{\chi(g)}$ for all $g \in G$, then $\chi^{-1}$ and $\overline{\chi}$ are the same function, and so we use $\chi^{-1}$ and $\overline{\chi}$ interchangeably. More details are given in the next section.

**Theorem 7.6.** *Let $G = \langle g_0 \rangle$ be a cyclic group of order $n$. Then the following statements hold.*

(i) *If a character $\chi$ of $G$ is given, then*

$$\sum_{g \in G} \chi(g) = \begin{cases} n, & \textit{if } \chi = \chi_0; \\ 0, & \textit{otherwise.} \end{cases}$$

(ii) *If $g \in G$ is given, then*

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} n, & \textit{if } g = 1; \\ 0, & \textit{otherwise.} \end{cases}$$

(iii) *$\widehat{G}$ is a cyclic group generated by $\chi_1$, where $\chi_1$ is the character defined in Theorem* 7.3.

**Proof.** For (i), let $\chi$ be a character of $G$. Then by Theorem 7.3, there exists $m = 0, 1, \ldots, n-1$ such that $\chi = \chi_m$ and

$$\sum_{g \in G} \chi(g) = \sum_{k=0}^{n-1} \chi_m(g_0^k) = \sum_{k=0}^{n-1} e\left(\frac{mk}{n}\right) = \sum_{k=0}^{n-1} \left(e\left(\frac{m}{n}\right)\right)^k .$$

This sum is a geometric progression which is equal to $n$ if $m = 0$, and is equal to 0 otherwise. The value $m = 0$ corresponds to the principal character $\chi_0$, so (i) is proved. For (ii), let $g = g_0^k$ for some $k = 0, 1, \ldots, n-1$. By Theorem 7.3, we obtain

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{m=0}^{n-1} \chi_m(g) = \sum_{m=0}^{n-1} \chi_m(g_0^k) = \sum_{m=0}^{n-1} e\left(\frac{mk}{n}\right),$$

which is equal to $n$ if $k = 0$ and is equal to 0 if $k \neq 0$. The value $k = 0$ corresponds to $g = 1$. This proves (ii). For (iii), we observe from Theorem 7.3 that

$$\widehat{G} = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\} = \{\chi_1^0, \chi_1, \chi_1^2, \ldots, \chi_1^{n-1}\} = \langle \chi_1 \rangle .$$

This completes the proof. □

Theorems 7.3 and 7.6 can be generalized to the case of a direct sum of cyclic groups. Recall that if $(G_1, *)$ and $(G_2, \circ)$ are groups, then the direct product of $G_1$ and $G_2$ is the set $G_1 \times G_2$ together with the pointwise multiplication defined by

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 * g_1', g_2 \circ g_2').$$

If $*$ and $\circ$ are commutative and written additively, then the direct product is called the direct sum and we sometimes write

$$G_1 \oplus G_2 \quad \text{instead of} \quad G_1 \times G_2.$$

Suppose that $G \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ and we would like to determine all characters $\chi$ of $G$. Since $(1, 0)$ has order $m$ and $(0, 1)$ has order $n$, we see that $\chi((1, 0))$ is an $m$th root of unity and $\chi((0, 1))$ is an $n$th root of unity, say

$$\chi(1, 0) = e\left(\frac{k_1}{m}\right), \quad \chi(0, 1) = e\left(\frac{k_2}{n}\right)$$

for some $0 \leq k_1 \leq m-1$ and $0 \leq k_2 \leq n-1$. Then

$$\chi((a,b)) = \chi(a(1,0)+b(0,1)) = \chi(1,0)^a\chi(0,1)^b = e\left(\frac{ak_1}{m}\right)e\left(\frac{bk_2}{n}\right).$$

Similar to the proof of Theorem 7.3, it can be checked that this gives a well-defined character on $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Since there are $m$ choices for $k_1$ and $n$ choices for $k_2$, there are $mn$ distinct characters of

$$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

We conclude that $G$ has exactly $mn$ characters $\chi_{k_1,k_2}$, where $k_1 = 0, 1, \ldots, m-1$ and $k_2 = 0, 1, \ldots, n-1$, given by

$$\chi_{k_1,k_2}((a,b)) = e\left(\frac{ak_1}{m}\right)e\left(\frac{bk_2}{n}\right)$$

for every $(a,b) \in \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. The same argument also gives us a complete list of characters of $G$ when

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$$

is any finite direct sum of cyclic groups. Combining with the following well-known result from algebra, we obtain a complete classification of all characters of any finite abelian group. We record them below.

**Theorem 7.7.** *Every finite abelian group is isomorphic to a direct sum of cyclic groups.*

**Proof.** This is well known. For the proof, see for example in [**107**]. ☐

**Theorem 7.8.** *Let $G$ be a finite abelian group of order $n$. Then $G$ has exactly $n$ characters. Moreover, let*

$$G = \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_\ell\mathbb{Z}.$$

*Then all characters of $G$ are of the form*

$$\chi((a_1, a_2, \ldots, a_\ell)) = e\left(\frac{a_1k_1}{m_1}\right)e\left(\frac{a_2k_2}{m_2}\right)\cdots e\left(\frac{a_\ell k_\ell}{m_\ell}\right)$$

*where $k_i$ ranges over $0, 1, \ldots, m_i - 1$ for each $i = 1, 2, \ldots, \ell$. In addition, $\widehat{G}$ is a finite abelian group of order $n$, $|\widehat{G}| = |G| = m_1m_2\cdots m_k$, and $\widehat{G}$ is isomorphic to $G$:*

$$\begin{aligned}\widehat{G} &\simeq \widehat{\mathbb{Z}/m_1\mathbb{Z}} \times \widehat{\mathbb{Z}/m_2\mathbb{Z}} \times \cdots \times \widehat{\mathbb{Z}/m_\ell\mathbb{Z}} \\ &\simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_\ell\mathbb{Z} \simeq G.\end{aligned} \tag{7.1}$$

**Proof.** We first consider the case when $G$ is the direct sum of $\mathbb{Z}/m_i\mathbb{Z}$. For each $i = 1, 2, 3, \dots, \ell$, let $e_i = (0, 0, \dots, 1, 0, 0, \dots, 0)$ where 1 is in the $i$th position. Then $e_i$ has order $m_i$ and $\chi(e_i)$ is an $m_i$th root of unity. Following the argument shown above, we obtain the desired formula for $\chi((a_1, a_2, \dots, a_\ell))$. From this formula, we also see that $\chi$ is a product of the characters of $\mathbb{Z}/m_1\mathbb{Z}, \dots, \mathbb{Z}/m_\ell\mathbb{Z}$. Therefore (7.1) holds and $|\widehat{G}| = |G| = m_1 m_2 \cdots m_k$. If $G$ is a finite abelian group, then we obtain by Theorem 7.7 that

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_\ell\mathbb{Z}.$$

The characters of $G$ have a one-to-one correspondence with those of $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_\ell\mathbb{Z}$, so the proof is complete. ☐

**Remark 7.9.** For our purpose, it may be unnecessary to use Theorem 7.8 since we only need to understand the characters of $(\mathbb{Z}/m\mathbb{Z})^\times$, the group of reduced residue classes mod $m$. In this case, we only need to use Theorems 7.3 to 7.6 and the Chinese remainder theorem: if $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the canonical factorization of $m$, then

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \oplus (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^\times \oplus \cdots \oplus (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times, \text{ and}$$

$$(\mathbb{Z}/p^a\mathbb{Z})^\times \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a-2}\mathbb{Z}, & \text{if } p = 2 \text{ and } a > 2; \\ \mathbb{Z}/(p-1)p^{a-1}\mathbb{Z}, & \text{otherwise.} \end{cases}$$

More properties of the characters are given in the next section.

## 7.2. The Orthogonality Relations

The characters of a finite abelian group $G$ satisfy the relations known as the orthogonality relations. When $G = (\mathbb{Z}/m\mathbb{Z})^\times$, these relations allow us to express the characteristic function of a reduced residue class modulo $m$ as a linear combination of characters. In fact, these are generalizations of Theorem 7.6. To prove them, we need the following lemma.

**Lemma 7.10.** *Let $G$ be a finite abelian group and let $g \neq 1$ be a nonidentity element of $G$. Then there exists $\psi \in \widehat{G}$ such that $\psi(g) \neq 1$.*

**Proof.** Let $f : G \to \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_\ell\mathbb{Z}$ be an isomorphism. The function $f$ exists by Theorem 7.7. We will find a character $\chi$ of this direct sum such that $\chi(f(g)) \neq 1$. Since $f$ is an isomorphism and $g$ is not the identity of $G$, $f(g) \neq (0, 0, 0, \dots, 0)$. Suppose that the $r$th component of $f(g)$ is not zero. We define a character $\chi$ of the direct sum by choosing $k_i = 0$ for $i \neq r$ and $k_r = 1$ in Theorem 7.8. Then $\chi(f(g)) = e(a_r/m_r)$ for some $a_r = 1, \dots, m_r - 1$. So $\chi(f(g)) \neq 1$. If $\psi = \chi \circ f$, then $\psi \in \widehat{G}$ and $\psi(g) \neq 1$, as required. □

**Theorem 7.11.** *Let G be a finite abelian group. Then the following statements hold.*

(i) *If a character $\chi$ of g is given, then*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{if } \chi = \chi_0; \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *If $g \in G$ is given, then*

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G|, & \text{if } g = 1; \\ 0, & \text{otherwise.} \end{cases}$$

**Proof.** If $\chi = \chi_0$ is given, then $\chi(g) = 1$ for all $g \in G$ and the sum in (i) is equal to $|G|$. Assume that $\chi \neq \chi_0$ is given and $S_\chi = \sum_{g \in G} \chi(g)$. Then there exists $h \in G$ such that $\chi(h) \neq 1$. Since $G$ is a group, $hg$ runs over all the elements of $G$ as g does. Therefore

$$\chi(h) S_\chi = \chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g) = S_\chi.$$

So $(\chi(h) - 1) S_\chi = 0$. Since $\chi(h) \neq 1$, we obtain $S_\chi = 0$, as required. The same argument also gives us a proof of (ii) but we need to apply Theorem 7.8 and Lemma 7.10 as follows. If $g = 1$, then $\chi(g) = 1$ for all $\chi \in \widehat{G}$ and the sum in (ii) is equal to $|\widehat{G}| = |G|$. Suppose that $g \neq 1$ and let $S_g = \sum_{\chi \in \widehat{G}} \chi(g)$. Then there exists $\psi \in \widehat{G}$ such that $\psi(g) \neq 1$. As $\chi$ runs over all elements of $\widehat{G}$, so does $\psi\chi$. Therefore

$$\psi(g) S_g = \psi(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} (\psi\chi)(g) = \sum_{\chi \in \widehat{G}} \chi(g) = S_g.$$

So $(\psi(g) - 1) S_g = 0$, which implies $S_g = 0$. This completes the proof. □

We recall from Remark 7.5 that if $G$ is a finite abelian group of order $n$, then $\chi(g)$ is an $n$th root of unity and therefore

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}.$$

By defining $\overline{\chi}(g) = \overline{\chi(g)}$, we see that $\chi^{-1} = \overline{\chi}$. With this observation, we obtain the following corollary.

**Corollary 7.12.** *Let G be a finite abelian group. Then the following holds.*

(i) *If $\chi$ and $\psi$ are characters of G, then*

$$\sum_{g\in G} \psi(g)\overline{\chi}(g) = \begin{cases} |G|, & \text{if } \psi = \chi; \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *If g and h are elements of G, then*

$$\sum_{\chi\in \widehat{G}} \chi(g)\overline{\chi}(h) = \begin{cases} |G|, & \text{if } g = h; \\ 0, & \text{otherwise.} \end{cases}$$

**Proof.** The sum in (i) can be written as $\sum_{g\in G}(\psi\chi^{-1})(g)$ and

$$\psi\chi^{-1} = \chi_0 \quad \text{if and only if} \quad \psi = \chi.$$

The sum in (ii) is equal to $\sum_{\chi\in\widehat{G}} \chi(gh^{-1})$. Therefore this corollary follows from Theorem 7.11. ☐

## 7.3. Dirichlet Characters

In this section, we focus our study on the characters of $(\mathbb{Z}/q\mathbb{Z})^\times$. Recall that the set of reduced residue classes modulo $q$:

$$(\mathbb{Z}/q\mathbb{Z})^\times = \{[a] \mid 1 \le a \le q \text{ and } (a,q) = 1\}$$

is a group under the multiplication given by $[a][b] = [ab]$. As usual, we sometimes write $\overline{a}$ or simply $a$ instead of $[a]$. Dirichlet characters are defined as follows.

**Definition 7.13.** Let $G = (\mathbb{Z}/q\mathbb{Z})^\times$ be the group of reduced residue classes modulo $q$. For each $f \in \widehat{G}$, define the function $\chi : \mathbb{N} \to \mathbb{C}$ by

$$\chi(n) = \begin{cases} f\big([n]\big), & \text{if } (n,q) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

The function $\chi$ is called a *Dirichlet character modulo q*. We also say that the character $f$ induces $\chi$ or the Dirichlet character $\chi$ is induced by $f$. In particular, the *principal Dirichlet character* $\chi_0$ is induced by the principal character of $(\mathbb{Z}/q\mathbb{Z})^\times$ and is given by

$$\chi_0(n) = \begin{cases} 1, & \text{if } (n,q) = 1; \\ 0, & \text{if } (n,q) > 1. \end{cases}$$

The following theorem gives a characterization of the Dirichlet characters.

**Theorem 7.14.** *Let $q \geq 1$ be an integer. Then there are exactly $\varphi(q)$ Dirichlet characters mod $q$ each of which is completely multiplicative and periodic with period $q$. That is, if $\chi$ is a Dirichlet character modulo $q$, then*

$$\chi(mn) = \chi(m)\chi(n) \quad \textit{and} \quad \chi(n+q) = \chi(n) \quad \textit{for all } m, n \in \mathbb{N}.$$

**Proof.** By Theorem 7.8, we know that $|G| = |\widehat{G}|$ for any finite abelian group $G$. Since $|(\mathbb{Z}/q\mathbb{Z})^\times| = \varphi(q)$, the number of characters of $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ is $\varphi(q)$. As in Definition 7.13, each Dirichlet character is induced by a unique character of $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$. So there are exactly $\varphi(q)$ Dirichlet characters modulo $q$. Next, let $\chi$ be a Dirichlet character modulo $q$ and let $m, n \in \mathbb{N}$. Let $f$ be the character of $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ which induces $\chi$, that is, for each $n \in \mathbb{N}$,

$$\chi(n) = \begin{cases} f\big([n]\big), & \text{if } (n,q) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

If $(m,q) > 1$ or $(n,q) > 1$, then $(mn,q) > 1$ and therefore $\chi(mn) = 0 = \chi(m)\chi(n)$. If $(m,q) = (n,q) = 1$, then $(mn,q) = 1$ and

$$\chi(m)\chi(n) = f\big([m]\big)f\big([n]\big) = f\big([m][n]\big) = f\big([mn]\big) = \chi(mn).$$

This shows that $\chi$ is completely multiplicative. Since $(n+q,q) = (n,q)$, we see that if $(n+q,q) = 1$, then $(n,q) = 1$ and $\chi(n+q) = f\big([n+q]\big) = f\big([n]\big) = \chi(n)$. Similarly, if $(n+q,q) > 1$, then $(n,q) > 1$ and $\chi(n+q) = 0 = \chi(n)$. Therefore $\chi$ is periodic with period $q$. This completes the proof. □

Let $\chi$ be a Dirichlet character modulo $q$ induced by $f \in \widehat{(\mathbb{Z}/q\mathbb{Z})^\times}$. If $(n,q) > 1$, then $\overline{\chi}(n) = \overline{\chi(n)} = 0$. If $(n,q) = 1$, then $|\chi(n)| = |f(n)| = 1$ and therefore

$$\overline{\chi}(n) = \overline{\chi(n)} = \chi(n)^{-1} = \chi(n^{-1}) = f(n^{-1}) = f^{-1}(n).$$

Thus $\overline{\chi}$ is a Dirichlet character mod $q$ induced by $f^{-1}$. Therefore the orthogonality relations previously obtained translate into the following theorems.

**Theorem 7.15.** *Let $q$ be a positive integer and let $\chi$, $\psi$ be Dirichlet characters modulo $q$. Then*

$$\sum_{a \bmod q} \psi(a)\overline{\chi}(a) = \begin{cases} \varphi(q), & \text{if } \psi = \chi; \\ 0, & \text{otherwise,} \end{cases}$$

*where $a$ runs over a complete residue modulo $q$.*

**Proof.** We first observe that $\psi$ and $\overline{\chi}$ have period $q$, so the sums taken over any complete residue modulo $q$ are the same. The index $a \bmod q$ of the sum can be replaced by $1 \le a \le q$, or $0 \le a \le q-1$, etc. If $(a, q) > 1$, then $\psi(a)\overline{\chi}(a) = 0$. So the sum reduces to $\sum_a \psi(a)\overline{\chi}(a)$ where $a$ runs over the elements of $(\mathbb{Z}/q\mathbb{Z})^\times$. Then by Corollary 7.12, the sum is equal to $|(\mathbb{Z}/q\mathbb{Z})^\times| = \varphi(q)$ if $\psi = \chi$ and is equal to 0 otherwise. ☐

Another form of the orthogonality relation is given below. See also Exercises 7.8.1 and 7.8.2 for interesting identities that can be obtained from the orthogonality relation.

**Theorem 7.16.** *Let $a$, $b$, and $q$ be positive integers and let $(a, q) = 1$. Then*

$$\sum_{\chi \bmod q} \chi(a)\overline{\chi}(b) = \begin{cases} \varphi(q), & \text{if } a \equiv b \pmod{q}; \\ 0, & \text{otherwise,} \end{cases}$$

*where $\chi$ runs over all Dirichlet characters modulo $q$.*

**Proof.** If $(b, q) > 1$, then $b \not\equiv a \pmod{q}$, $\overline{\chi}(b) = 0$, and the sum is zero. So assume that $(b, q) = 1$. Each $\chi$ is induced by a unique character $f$ of $(\mathbb{Z}/q\mathbb{Z})^\times$ and $\chi(a)\overline{\chi}(b)$ is equal to $f(a)f^{-1}(b)$. So we can write the sum as $\sum_{\chi \in \hat{G}} \chi(a)\overline{\chi}(b)$ where $G = (\mathbb{Z}/q\mathbb{Z})^\times$ and apply Corollary 7.12 to obtain the desired result. ☐

Next, we give some examples to illustrate basic calculations in the Dirichlet characters.

**Example 7.17.** The following tables essentially display all values of the Dirichlet characters modulo $q$ for $q = 1, 2, 3, 4, 5$.

| $n$ | 1 |
|---|---|
| $\chi_0(n)$ | 1 |

$q = 1, \varphi(q) = 1$

| $n$ | 1 | 2 |
|---|---|---|
| $\chi_0(n)$ | 1 | 0 |

$q = 2, \varphi(q) = 1$

| $n$ | 1 | 2 | 3 |
|---|---|---|---|
| $\chi_0(n)$ | 1 | 1 | 0 |
| $\chi_1(n)$ | 1 | $-1$ | 0 |

$q = 3, \varphi(q) = 2$

| $n$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $\chi_0(n)$ | 1 | 0 | 1 | 0 |
| $\chi_1(n)$ | 1 | 0 | $-1$ | 0 |

$q = 4, \varphi(q) = 2$

| $n$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $\chi_0(n)$ | 1 | 1 | 1 | 1 | 0 |
| $\chi_1(n)$ | 1 | $-1$ | $-1$ | 1 | 0 |
| $\chi_2(n)$ | 1 | $i$ | $-i$ | $-1$ | 0 |
| $\chi_3(n)$ | 1 | $-i$ | $i$ | $-1$ | 0 |

$q = 5, \varphi(q) = 4$

To fill in these tables, we use the fact that

$$\chi(n)^{\varphi(q)} = 1 \text{ whenever } (n, q) = 1,$$

so $\chi(n)$ is a $\varphi(q)$th root of unity. For instance, consider when $q = 5$. Then $\varphi(q) = 4$ and there are four Dirichlet characters $\chi_0, \chi_1, \chi_2, \chi_3$. Since $3^2 \equiv 4$, $3^3 \equiv 2$, $3^4 \equiv 1 \pmod 5$, $\chi(3) = 1, -1, i, -i$ and $\chi$ is completely determined by $\chi(3)$.

**Example 7.18.** The following tables show all the Dirichlet characters mod $q$ for $q = 8, 9, 10$.

If $q = 8$, then $\varphi(q) = 4$ and so there are four Dirichlet characters $\chi_0, \chi_1, \chi_2, \chi_3$. In addition, $3^2 \equiv 1 \pmod 8$, and $5^2 \equiv 1 \pmod 8$. So $\chi(3) = 1, -1$, $\chi(5) = 1, -1$. Since $3 \cdot 5 \equiv 7 \pmod 8$, $\chi(3)\chi(5) = \chi(7)$. So $\chi(7)$ is determined by $\chi(3)$ and $\chi(5)$. This gives the tables of all the Dirichlet characters mod $q$ for $q = 8$ as follows.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\chi_0(n)$ | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| $\chi_1(n)$ | 1 | 0 | 1 | 0 | $-1$ | 0 | $-1$ | 0 |
| $\chi_2(n)$ | 1 | 0 | $-1$ | 0 | 1 | 0 | $-1$ | 0 |
| $\chi_3(n)$ | 1 | 0 | $-1$ | 0 | $-1$ | 0 | 1 | 0 |

$q = 8, \varphi(q) = 4$

For $q = 9$, we have $\varphi(q) = 6$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1 \pmod 9$. So $\chi(2)^6 = 1$ and $\chi$ is uniquely determined by $\chi(2)$. Let $\omega = e\left(\frac{1}{6}\right)$. Then $\omega^3 = -1$, $\omega^4 = -\omega$, $\omega^5 = -\omega^2$. All six Dirichlet characters mod 9 are shown below.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| $\chi_0(n)$ | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| $\chi_1(n)$ | 1 | $\omega^2$ | 0 | $-\omega$ | $-\omega$ | 0 | $\omega^2$ | 1 | 0 |
| $\chi_2(n)$ | 1 | $-1$ | 0 | 1 | $-1$ | 0 | 1 | $-1$ | 0 |
| $\chi_3(n)$ | 1 | $-\omega$ | 0 | $\omega^2$ | $\omega^2$ | 0 | $-\omega$ | 1 | 0 |
| $\chi_4(n)$ | 1 | $-\omega^2$ | 0 | $-\omega$ | $\omega$ | 0 | $\omega^2$ | $-1$ | 0 |
| $\chi_5(n)$ | 1 | $\omega$ | 0 | $\omega^2$ | $-\omega^2$ | 0 | $-\omega$ | $-1$ | 0 |

$q = 9, \varphi(q) = 6$

For $q = 10$, we have $\varphi(q) = 4$, $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 7$, $3^4 \equiv 1 \pmod{10}$. So $\chi(3) = 1, -1, i, -i$ and $\chi$ is uniquely determined by $\chi(3)$. All four Dirichlet characters mod 10 are given in the following table.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\chi_0(n)$ | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| $\chi_1(n)$ | 1 | 0 | $-1$ | 0 | 0 | 0 | $-1$ | 0 | 1 | 0 |
| $\chi_2(n)$ | 1 | 0 | $i$ | 0 | 0 | 0 | $-i$ | 0 | $-1$ | 0 |
| $\chi_3(n)$ | 1 | 0 | $-i$ | 0 | 0 | 0 | $i$ | 0 | $-1$ | 0 |

$q = 10, \varphi(q) = 4$

Certain sums involving the Dirichlet characters are given in the next section and in the exercise.

## 7.4. Dirichlet $L$-Functions

In this section, we give some results on the sums involving $\chi(n)$. In particular, we focus on showing the nonvanishing of

$$\sum_{n=1}^{\infty} \chi(n)/n,$$

which is a major step in proving Dirichlet's theorem. In fact, the sum $\sum_{n=1}^{\infty} \chi(n)/n$ belongs to a class of Dirichlet $L$-series.

**Definition 7.19.** Let $\chi$ be a Dirichlet character modulo $q$. The *Dirichlet L-series associated with* $\chi$ (also called a *Dirichlet L-function modulo* $q$) is the series (the function) of the form

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

**Theorem 7.20.** *Let $\chi$ be a nonprincipal Dirichlet character* mod $q$ *and let $f$ be a positive function that has a continuous negative derivative. Then*

$$\sum_{x<n\le y} \chi(n)f(n) = O(f(x)).$$

*In addition, if $f(x) \to 0$ as $x \to \infty$, then the series $\sum_{n=1}^{\infty} \chi(n)f(n)$ converges and we have*

$$\sum_{n\le x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O\big(f(x)\big).$$

**Proof.** Let $A(x) = \sum_{n\le x} \chi(n)$. Since $\chi$ is a nonprincipal character, we obtain that $\sum_{n=1}^{q} \chi(n) = 0$, and in general, $\sum_{n=1}^{kq} \chi(n) = 0$ for every $k \in \mathbb{N}$. Therefore we obtain

$$|A(x)| \le \sum_{n=1}^{q} |\chi(n)| = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} 1 = \varphi(q) = O(1), \quad \text{and}$$

$$\begin{aligned} \sum_{x<n\le y} \chi(n)f(n) &= \int_x^y f(t)\, dA(t) \\ &= A(y)f(y) - A(x)f(x) - \int_x^y A(t)f'(t)\, dt \\ &\ll f(y) + f(x) + \int_x^y |f'(t)|\, dt \ll f(x). \end{aligned}$$

Next, assume that $f(x) \to 0$ as $x \to \infty$. Since

$$\sum_{N<n\le M} \chi(n)f(n) \ll f(N),$$

the sum converges to 0 as $M, N \to \infty$, so the series $\sum_{n=1}^{\infty} \chi(n) f(n)$ converges by the Cauchy criterion. Then

$$\begin{aligned}\sum_{n\leqslant x} \chi(n)f(n) &= \sum_{n=1}^{\infty} \chi(n)f(n) - \sum_{n>x} \chi(n)f(n)\\ &= \sum_{n=1}^{\infty} \chi(n)f(n) - \lim_{y\to\infty}\Bigg(\sum_{x<n\leqslant y} \chi(n)f(n)\Bigg)\\ &= \sum_{n=1}^{\infty} \chi(n)f(n) + O\big(f(x)\big).\end{aligned}$$

This completes the proof. □

**Theorem 7.21.** *Let $\chi$ be a nonprincipal Dirichlet character modulo $q$. Then for all $x \geqslant 2$, we have*

$$\sum_{n\leqslant x} \frac{\chi(n)}{n} = L(1,\chi) + O\left(\frac{1}{x}\right),$$

$$\sum_{n\leqslant x} \frac{\chi(n)\log n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} + O\left(\frac{\log x}{x}\right),$$

$$\sum_{n\leqslant x} \frac{\chi(n)}{\sqrt{n}} = L\left(\frac{1}{2},\chi\right) + O\left(\frac{1}{\sqrt{x}}\right).$$

**Proof.** Applying Theorem 7.20 with $f(x) = \frac{1}{x}$, $f(x) = \frac{\log x}{x}$, and $f(x) = \frac{1}{\sqrt{x}}$, respectively, we obtain the desired result. □

If $\chi(n) \in \mathbb{R}$ for all $n \in \mathbb{N}$, then $\chi$ is called a *real character*. If $\chi$ is a principal character mod $q$, then it is not difficult to see that $L(1,\chi)$ diverges to $\infty$, so it is not zero. Next, we show that $L(1,\chi) \neq 0$ when $\chi$ is a real nonprincipal Dirichlet character modulo $q$.

**Theorem 7.22.** *Let $\chi$ be a real nonprincipal Dirichlet character* mod $q$*, $r(n) = \sum_{d\mid n} \chi(d)$, and $A(x) = \sum_{n\leqslant x} \frac{r(n)}{\sqrt{n}}$. Then the following statements hold.*

(i) *$r(n) \geq 0$ for all $n \in \mathbb{N}$ and $r(n) \geq 1$ if $n$ is a square.*

(ii) *$A(x) \to \infty$ as $x \to \infty$.*

(iii) *$A(x) = 2\sqrt{x}\,L(1,\chi) + O(1)$.*

(iv) *$L(1,\chi) \neq 0$.*

**Proof.** Since $\chi$ is multiplicative, we obtain that $r$ is multiplicative too and it is enough to consider $r(n)$ when $n$ is a power of a prime. In addition, $\chi$ is real and $\chi(n)$ is either zero or a root of unity, so $\chi(n) = 0$ or $\pm 1$ for each $n \in \mathbb{N}$. Let $p$ be a prime and $a \geq 1$. Then $r(p^a)$ is equal to

$$\begin{aligned}\sum_{d|p^a} \chi(d) &= \chi(1) + \chi(p) + \chi(p^2) + \cdots + \chi(p^a) \\ &= 1 + \chi(p) + \chi(p)^2 + \cdots + \chi(p)^a \\ &= \begin{cases} a+1, & \text{if } \chi(p) = 1; \\ 1, & \text{if } \chi(p) = 0 \text{ or if } \chi(p) = -1 \text{ and } a \text{ is even;} \\ 0, & \text{if } \chi(p) = -1 \text{ and } a \text{ is odd.} \end{cases}\end{aligned}$$

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Then $r(n) = r(p_1^{a_1}) r(p_2^{a_2}) \cdots r(p_k^{a_k}) \geq 0$. If $n$ is a square, then $a_1, a_2, \ldots, a_k$ are even, $r(p_i^{a_i}) \geq 1$ for all $i$, and therefore $r(n) \geq 1$. This proves (i). For (ii), we obtain from (i) that $A(x)$ is larger than or equal to

$$\begin{aligned}\sum_{\substack{n \leq x \\ n \text{ is a square}}} \frac{1}{\sqrt{n}} = \sum_{m^2 \leq x} \frac{1}{\sqrt{m^2}} &= \sum_{m \leqslant \sqrt{x}} \frac{1}{m} \\ &= \log \sqrt{x} + \gamma + O\left(\frac{1}{\sqrt{x}}\right),\end{aligned}$$

which implies that $A(x) \to \infty$ as $x \to \infty$. Next, we prove (iii). By changing the order of summation and applying Dirichlet's hyperbola method, we obtain

$$\begin{aligned}A(x) &= \sum_{n \leq x} \sum_{d|n} \frac{\chi(d)}{\sqrt{n}} = \sum_{dk \leq x} \frac{\chi(d)}{\sqrt{dk}} \\ &= \sum_{d \leq \sqrt{x}} \sum_{k \leq \frac{x}{d}} \frac{\chi(d)}{\sqrt{dk}} + \sum_{k \leq \sqrt{x}} \sum_{d \leq \frac{x}{k}} \frac{\chi(d)}{\sqrt{dk}} - \sum_{k \leq \sqrt{x}} \sum_{d \leq \sqrt{x}} \frac{\chi(d)}{\sqrt{dk}} \\ &= \sum_{d \leq \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{k \leq \frac{x}{d}} \frac{1}{\sqrt{k}} + \sum_{k \leq \sqrt{x}} \frac{1}{\sqrt{k}} \sum_{d \leq \frac{x}{k}} \frac{\chi(d)}{\sqrt{d}} \\ &\quad - \sum_{k \leq \sqrt{x}} \frac{1}{\sqrt{k}} \sum_{d \leq \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \\ &= S_1 + S_2 - S_3, \text{ say.}\end{aligned}$$

Recall that if $0 < s < 1$, then

$$\sum_{n \le x} \frac{1}{n^s} = \frac{x^{-s+1}}{-s+1} + a + O\left(\frac{1}{x^s}\right) = \frac{x^{-s+1}}{-s+1} + O(1),$$

where $a = \zeta(s)$ is a constant. By this formula and Theorem 7.21, we obtain

$$\begin{aligned}
S_1 &= \sum_{d \leqslant \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \left(2\left(\frac{x}{d}\right)^{\frac{1}{2}} + a + O\left(\left(\frac{d}{x}\right)^{\frac{1}{2}}\right)\right) \\
&= 2\sqrt{x} \sum_{d \leqslant \sqrt{x}} \frac{\chi(d)}{d} + a \sum_{d \leqslant \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} + O\left(\frac{1}{\sqrt{x}} \sum_{d \leqslant \sqrt{x}} |\chi(d)|\right) \\
&= 2\sqrt{x}\left(L(1,\chi) + O\left(x^{-\frac{1}{2}}\right)\right) + a\left(L(1/2,\chi) + O\left(x^{-\frac{1}{4}}\right)\right) + O(1) \\
&= 2\sqrt{x}\, L(1,\chi) + aL(1/2,\chi) + O(1) = 2\sqrt{x}L(1,\chi) + O(1).
\end{aligned}$$

Similarly, we obtain

$$\begin{aligned}
S_2 &= \sum_{k \leqslant \sqrt{x}} \frac{1}{\sqrt{k}} \left(L(1/2,\chi) + O\left(\sqrt{\frac{k}{x}}\right)\right) \\
&= L(1/2,\chi)\left(2\sqrt{x}^{\frac{1}{2}} + O(1)\right) + O(1) = 2x^{\frac{1}{4}} L(1/2,\chi) + O(1), \\
S_3 &= \left(2x^{\frac{1}{4}} + O(1)\right)\left(L(1/2,\chi) + O\left(x^{-\frac{1}{4}}\right)\right) \\
&= 2x^{\frac{1}{4}} L(1/2,\chi) + O(1).
\end{aligned}$$

Hence $S_1 + S_2 - S_3 = 2\sqrt{x}\, L(1,\chi) + O(1)$, which proves (iii). If $L(1,\chi) = 0$, then $A(x) = O(1)$ which contradicts (ii). So $L(1,\chi) \neq 0$, as required. □

## 7.5. Dirichlet's Theorem

Before proceeding to the next step, let us review what we have previously done. We introduced the concept of characters of a group in Section 7.1 and proved their orthogonality relations in Section 7.2. After that, we gave the definition of Dirichlet characters and Dirichlet $L$-functions in Sections 7.3 and 7.4, respectively. We obtained the orthogonality relations for Dirichlet characters in Theorem 7.16 and the nonvanishing of $L(1,\chi)$ for all real nonpricipal Dirichlet characters $\chi$ in Theorem 7.22.

All of these are preliminary to the proof of Dirichlet's theorem as follows.

**Theorem 7.23.** (Dirichlet's Theorem) *Let* $a, q \in \mathbb{N}$ *and* $(a,q)=1$. *Then*

$$\sum_{\substack{p \le x \\ p \equiv a \pmod q}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O(1).$$

*In particular, there are infinitely many primes* $p \equiv a \pmod q$*.*

**Proof.** The proof consists of several steps as follows.

**Step 1** We show that

$$\sum_{\substack{p \le x \\ p \equiv a \pmod q}} \frac{\log p}{p} = \sum_{\substack{n \le x \\ n \equiv a \pmod q}} \frac{\Lambda(n)}{n} + O(1). \tag{7.2}$$

Consider

$$\begin{aligned} \sum_{\substack{n \le x \\ n \equiv a \pmod q}} \frac{\Lambda(n)}{n} &= \sum_{\substack{p^k \le x \\ p^k \equiv a \pmod q}} \frac{\log p}{p^k} \\ &= \sum_{\substack{p \le x \\ p \equiv a \pmod q}} \frac{\log p}{p} + \sum_{\substack{p^k \le x \\ k \ge 2 \\ p^k \equiv a \pmod q}} \frac{\log p}{p^k}. \end{aligned}$$

The second term above is less than or equal to

$$\sum_{\substack{p^k \le x \\ k \ge 2}} \frac{\log p}{p^k} \le \sum_{p \le \sqrt{x}} \log p \sum_{k=2}^{\infty} \frac{1}{p^k} \le \sum_{p} \frac{\log p}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} \ll 1.$$

This proves (7.2).

**Step 2** We capture the condition $p \equiv a \pmod q$ by the orthogonality relation of the characters modulo $q$. Recall that for $(m,q)=1$, we have

$$\sum_{\chi \bmod q} \chi(k)\overline{\chi}(m) = \begin{cases} \varphi(q), & \text{if } k \equiv m (\bmod q); \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} \frac{\Lambda(n)}{n} = \sum_{n\le x} \frac{\Lambda(n)}{n}\left(\frac{1}{\varphi(q)}\sum_{\chi \bmod q} \chi(n)\overline{\chi}(a)\right)$$

$$= \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi}(a) \sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n}. \tag{7.3}$$

We expect some cancellations arising from the nonprincipal characters and the main term should come from the contribution of $\chi_0$. So we first consider

$$\sum_{n\le x} \frac{\chi_0(n)\Lambda(n)}{n} = \sum_{\substack{n\le x\\ (n,q)=1}} \frac{\Lambda(n)}{n} = \sum_{n\le x} \frac{\Lambda(n)}{n} - \sum_{\substack{n\le x\\ (n,q)>1}} \frac{\Lambda(n)}{n}$$

$$= \log x - \sum_{\substack{p^k\le x\\ p\mid q}} \frac{\log p}{p^k} + O(1).$$

The sum above is

$$\le \sum_{p\mid q} \frac{\log p}{p} + \sum_{p\mid q} \log p \sum_{k=2}^{\infty} \frac{1}{p^k} = \sum_{p\mid q} \frac{\log p}{p-1} = O(1),$$

where the implied constant may depend on $q$. Therefore

$$\sum_{n\le x} \frac{\chi_0(n)\Lambda(n)}{n} = \log x + O(1). \tag{7.4}$$

Substituting (7.4) in (7.3), we obtain

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} \frac{\Lambda(n)}{n} \tag{7.5}$$

$$= \frac{1}{\varphi(q)} \log x + \frac{1}{\varphi(q)} \sum_{\substack{\chi \bmod q\\ \chi\ne\chi_0}} \overline{\chi}(a) \sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} + O(1).$$

So it remains to show that the second term on the right side of (7.5) is $O(1)$.

**Step 3** We show that if $\chi \ne \chi_0$, then

$$\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} = \begin{cases} O(1), & \text{if } L(1,\chi)\ne 0;\\ -\log x + O(1), & \text{otherwise.}\end{cases} \tag{7.6}$$

**Step 3.1** Suppose $\chi \neq \chi_0$ and $L(1,\chi) \neq 0$. Consider the sum

$$\sum_{n\le x} \frac{\chi(n)\log n}{n} = \sum_{n\le x} \frac{\chi(n)}{n} \sum_{d|n} \Lambda(d) = \sum_{dk\le x} \frac{\chi(dk)}{dk}\Lambda(d).$$

Since $\chi$ is completely multiplicative, the summand can be written as

$$\frac{\chi(d)\Lambda(d)}{d} \cdot \frac{\chi(k)}{k},$$

and for $d \le x$, we have

$$\sum_{k\le \frac{x}{d}} \frac{\chi(k)}{k} = L(1,\chi) + O\left(\frac{d}{x}\right),$$

by Theorem 7.21. Therefore the above sum is equal to

$$L(1,\chi)\sum_{d\le x} \frac{\chi(d)\Lambda(d)}{d} + O\left(\frac{1}{x}\sum_{d\le x}\Lambda(d)\right)$$
$$= L(1,\chi)\sum_{d\le x} \frac{\chi(d)\Lambda(d)}{d} + O(1).$$

By Theorem 7.21,

$$\sum_{n\le x} \frac{\chi(n)\log n}{n} \ll 1.$$

Therefore

$$L(1,\chi)\sum_{d\le x} \frac{\chi(d)\Lambda(d)}{d} = O(1).$$

Since $L(1,\chi) \neq 0$, we see that $\sum_{d\le x} \frac{\chi(d)\Lambda(d)}{d} = O(1)$, as required. We remark that the implicit constant above may depend on $\chi$ but the number of Dirichlet characters modulo $q$ is finite, so we may choose the implicit constant to depend only on $q$.

**Step 3.2** Assume that $\chi \neq \chi_0$ and $L(1,\chi) = 0$. Recall the identities

$$\Lambda(n) = \sum_{d|n} \mu(d)\log\frac{n}{d} = -\sum_{d|n}\mu(d)\log d.$$

Then

$$\sum_{d|n}\mu(d)\log\frac{x}{d} = (\log x)\sum_{d|n}\mu(d) - \sum_{d|n}\mu(d)\log d = \begin{cases} \log x, & \text{if } n = 1; \\ \Lambda(n), & \text{if } n > 1. \end{cases}$$

It follows that

$$\begin{aligned}\log x + \sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} &= \sum_{n\le x}\frac{\chi(n)}{n}\sum_{d|n}\mu(d)\log\frac{x}{d}\\ &= \sum_{d\le x}\mu(d)\log\frac{x}{d}\sum_{\substack{n\le x\\ d|n}}\frac{\chi(n)}{n} = \sum_{d\le x}\mu(d)\left(\log\frac{x}{d}\right)\frac{\chi(d)}{d}\sum_{k\le\frac{x}{d}}\frac{\chi(k)}{k}\\ &= L(1,\chi)\sum_{d\le x}\mu(d)\left(\log\frac{x}{d}\right)\frac{\chi(d)}{d} + O\left(\frac{1}{x}\sum_{d\le x}\log\frac{x}{d}\right) = O(1).\end{aligned}$$

Therefore $\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = -\log x + O(1)$. This completes the proof of (7.6).

**Step 4** We show that if $\chi$ is not a real character, then $L(1,\chi)\neq 0$. Let $N$ be the number of nonprincipal characters $\chi$ with $L(1,\chi)=0$. Then from (7.4) and (7.6), we obtain

$$\sum_{\chi \bmod q}\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = (1-N)\log x + O(1). \tag{7.7}$$

By the orthogonality relation, the left-hand side of (7.7) is

$$\sum_{n\le x}\frac{\Lambda(n)}{n}\sum_{\chi \bmod q}\chi(n) = \varphi(q)\sum_{\substack{n\le x\\ n\equiv 1 \pmod q}}\frac{\Lambda(n)}{n}\ge 0.$$

If $N>1$, then the right-hand side of (7.7) is negative for a large value of $x$ while the left-hand side of (7.7) is always nonnegative, a contradiction. Therefore $N\le 1$. Suppose for a contradiction that there exists a nonreal character $\chi$ such that $L(1,\chi)=0$. Then

$$L(1,\overline{\chi}) = \sum_{n=1}^{\infty}\frac{\overline{\chi}(n)}{n} = \overline{\sum_{n=1}^{\infty}\frac{\chi(n)}{n}} = \overline{L(1,\chi)} = 0.$$

Since $\chi$ is not real, $\chi\neq\overline{\chi}$. This shows that $N\ge 2$, which is a contradiction.

**Step 5** We give the proof of the theorem. By Theorem 7.22, we obtain that $L(1,\chi)\neq 0$ if $\chi$ is a real character. Combining this with the result in Step 4, we conclude that $L(1,\chi)\neq 0$ for every nonprincipal character $\chi$. By (7.6), we have

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = O(1) \quad \text{for every } \chi\neq\chi_0. \tag{7.8}$$

Then the desired result follows from (7.5) and (7.2). ☐

We also obtain the following results from the proof of Dirichlet's theorem.

**Theorem 7.24.** *Let $a$ and $q$ be positive integers and $(a, q) = 1$. Then the following statements hold.*

(i) $$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)}\log x + O(1).$$

(ii) $L(1,\chi) \neq 0$ *for every nonprincipal Dirichlet character* $\chi$.

(iii) $$\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} = \begin{cases} \log x + O(1), & \text{if } \chi = \chi_0; \\ O(1), & \text{if } \chi \neq \chi_0. \end{cases}$$

**Proof.** The statement (i) is obtained from (7.5) and (7.8), (ii) is from Step 5, and (iii) follows from (7.4) and (7.8). ☐

**Corollary 7.25.** *Let $a, q \in \mathbb{N}$ and $(a, q) = 1$. Then for $x \geq 2$, we have*

(i) $$\sum_{\substack{p\le x\\ p\equiv a \pmod q}} \frac{1}{p} = \frac{1}{\varphi(q)}\log\log x + A + O\left(\frac{1}{\log x}\right),$$

(ii) $$\prod_{\substack{p\le x\\ p\equiv a \pmod q}} \left(1-\frac{1}{p}\right)^{-1} = B(\log x)^{\frac{1}{\varphi(q)}}\left(1+O\left(\frac{1}{\log x}\right)\right),$$

*where $A$ and $B$ are constants depending at most on $a$ and $q$.*

**Proof.** For (i), we write

$$\frac{1}{p} = \left(\frac{\log p}{p}\right)\left(\frac{1}{\log p}\right)$$

and use partial summation to obtain that the sum is equal to

$$\int_{2^-}^{x} \frac{1}{\log t}dA(t) = \frac{A(x)}{\log x} + \int_{2}^{x} \frac{A(t)}{t(\log t)^2}dt, \tag{7.9}$$

where

$$A(t) = \sum_{\substack{p\le t\\ p\equiv a \pmod q}} \frac{\log p}{p} = \frac{\log x}{\varphi(q)} + R(t) \text{ and } R(t) = O(1).$$

Then (7.9) is equal to

$$\begin{aligned}\frac{1}{\varphi(q)} + \frac{1}{\varphi(q)}\int_2^x \frac{1}{t\log t}dt + \int_2^x \frac{R(t)}{t(\log t)^2}dt + O\left(\frac{1}{\log x}\right)\\ = \frac{1}{\varphi(q)}\log\log x + A + O\left(\frac{1}{\log x}\right)\end{aligned}$$

where $A = \frac{1}{\varphi(q)} - \frac{\log\log 2}{\varphi(q)} + \int_2^\infty \frac{R(t)}{t(\log t)^2}dt$. This proves (i). For (ii), we consider the logarithm of the product which is equal to

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv a \pmod q}} \log\left(1-\frac{1}{p}\right)^{-1} &= \sum_{\substack{p\le x\\ p\equiv a \pmod q}} \sum_{n=1}^{\infty} \frac{1}{np^n}\\ &= \sum_{\substack{p\le x\\ p\equiv a \pmod q}} \frac{1}{p} + \sum_{\substack{p\le x\\ p\equiv a \pmod q}} \sum_{n=2}^{\infty} \frac{1}{np^n}.\end{aligned}$$

The second sum is less than

$$\sum_{p\le x}\sum_{n=2}^{\infty}\frac{1}{p^n} = \sum_{p\le x}\frac{1}{p(p-1)} \le \sum_{n\le x}\frac{1}{n(n-1)} \ll \frac{1}{x}.$$

The first sum is obtained from (i). Therefore the product in (ii) is equal to

$$\begin{aligned}e^{\frac{1}{\varphi(q)}\log\log x + A + O\left(\frac{1}{\log x}\right)} &= (\log x)^{\frac{1}{\varphi(q)}} \cdot e^A \cdot e^{O\left(\frac{1}{\log x}\right)}\\ &= e^A(\log x)^{\frac{1}{\varphi(q)}}\left(1 + O\left(\frac{1}{\log x}\right)\right). \qquad \square\end{aligned}$$

## 7.6. Applications of Dirichlet's Theorem

In this section, we give various examples concerning arithmetic progressions and some integer sequences. Some of these problems may be easily solved by applying Dirichlet's theorem but, if it is possible, the reader should also try to solve them by a more elementary method. Throughout Examples 7.26 to 7.31, let $a$ and $q$ be positive integers, $(a,q)=1$, and let $A(a,q)$ be the set of all positive integers $n$ such that $n \equiv a \pmod q$.

**Example 7.26.** Let $m \ge 1$ be an integer. Show that $A(a,q)$ contains an integer relatively prime to $m$.

**Solution 1.** By Dirichlet's theorem, there are infinitely many primes $p \equiv a \pmod{q}$ and when $p > m$, we also have $(p, m) = 1$.

**Solution 2.** Let $S = \{a + tq \mid t = 1, 2, 3, \ldots, m\}$ and $k = mq$. By Theorem 1.24, there are $\varphi(k)/\varphi(q)$ elements of $S$ which are relatively prime to $k$. Let $n$ be such an element of $S$. Then $n \in A(a, q)$ and $(n, m) \leq (n, k) = 1$.

**Solution 3.** We construct $x, y \in \mathbb{N}$ such that $a + xq \equiv y \pmod{m}$ and $(y, m) = 1$. The integer $x$ exists if $(q, m) \mid y - a$. So $y = a + (q, m)j$ and we need to find $j \in \mathbb{N}$ such that $(a + (q, m)j, m) = 1$. Let $p \mid m$. If $p \mid a$, then $p \nmid q$ and if we choose $j$ so that $p \nmid j$, then $a + (q, m)j \equiv (q, m)j \not\equiv 0 \pmod{p}$. If $p \nmid a$, then we can choose $j$ so that $p \mid j$ and $a + (q, m)j \equiv a \not\equiv 0 \pmod{p}$. Therefore we would like to find $j$ such that (i) if $p \mid m$ and $p \mid a$, then $p \nmid j$, (ii) if $p \mid m$ and $p \nmid a$, then $p \mid j$. Therefore, we let

$$j = \left(1 + \prod_{p \mid (a,m)} p\right)\left(\prod_{p \mid m, p \nmid a} p\right).$$

If $p \mid m$, then $p \nmid y$ and so $(y, m) = 1$, as required. □

**Example 7.27.** Let $m \in \mathbb{N}$. Show that $A(a, q)$ contains infinitely many numbers relatively prime to $m$.

**Solution.** If $(a + xq, m) = 1$, then $(a + (x + \ell m)q, m) = 1$ for any $\ell \in \mathbb{N}$. So if there is an integer $n \in A(a, q)$ with $(n, m) = 1$, then there are infinitely many such $n$. So this result follows from Example 7.26. □

**Example 7.28.** Prove that $A(a, q)$ contains an infinite subset

$$\{a_1, a_2, \ldots\} \quad \text{such that } (a_i, a_j) = 1 \text{ if } i \neq j.$$

**Solution.** Again, this follows immediately from Dirichlet's theorem but we can construct $a_1, a_2, a_3, \ldots$ by applying the result in Example 7.26 too. Choose $a_1 = a$. There is $a_2 \in A(a, q)$ such that $(a_2, a_1) = 1$. For $m = a_1 a_2$, there is $a_3 \in A(a, q)$ such that $(a_3, m) = 1$. So $(a_3, a_1) = (a_3, a_2) = 1$. In general, if $a_1, a_2, \ldots, a_\ell$ are chosen, we let $m = a_1 a_2 \cdots a_\ell$ and choose $a_{\ell+1} \in A(a, q)$ such that $(a_{\ell+1}, m) = 1$. This shows that $A(a, q)$ contains an infinite subset $\{a_1, a_2, \ldots\}$ such that $(a_i, a_j) = 1$ if $i \neq j$. □

**Example 7.29.** Show that $A(a, q)$ contains infinitely many perfect squares if and only if $A(a, q)$ contains a square. Give an example of

$A(a,q)$ containing a perfect square and an example of $A(a,q)$ that does not contain any square.

**Solution.** If $m^2 \equiv a \pmod{q}$, then $(m+\ell q)^2 \equiv a \pmod{q}$ for any $\ell \in \mathbb{N}$. So the first statement is proved. If $a$ is a quadratic residue mod $q$, for instance, $a = 1$ and $q = 5$, then $A(a,q)$ contains a square. Similarly, if $a$ is a quadratic nonresidue modulo $q$ (such as $a = 2$ and $q = 5$), then $A(a,q)$ does not contain a square. ☐

**Example 7.30.** Prove that $A(a,q)$ contains an infinite subset that forms a geometric progression. Deduce that $A(a,q)$ contains infinitely many numbers having the same prime factors.

**Solution.** The numbers $a(q+1), a(q+1)^2, a(q+1)^3, \ldots$ form a geometric progression, each term is congruent to $a$ modulo $q$, and they all have the same prime factors as $a(q+1)$. ☐

**Example 7.31.** Let $S$ be an infinite subset of $A(a,q)$ and $n \in \mathbb{N}$. Show that $A(a,q)$ contains an element that can be expressed as a product of more than $n$ different elements of $S$.

**Solution.** It is enough to show that there are $s_1, s_2, \ldots, s_\ell \in S$, where $\ell > n$ such that $s_1 s_2 \cdots s_\ell \in A(a,q)$. Let $\ell \in \mathbb{N}$ be a number to specified later. Consider

$$s_1 s_2 \cdots s_\ell = (a+qx_1)(a+qx_2)\cdots(a+qx_\ell) = a^\ell + qy$$

for some $y \in \mathbb{N}$. We would like $a^\ell + qy \equiv a \pmod{q}$. Since $(a,q) = 1$, $a^{\varphi(q)} \equiv 1 \pmod{q}$. So for each $m \in \mathbb{N}$, we let $\ell = m\varphi(q) + 1$, so that $a^\ell + qy \equiv a \pmod{q}$. If $m$ is large enough, then $\ell > n$ and $a^\ell + qy \equiv a \pmod{q}$, as required. ☐

**Example 7.32.** Dirichlet's theorem implies the following statement: if $a$ and $q$ are positive integers and $(a,q) = 1$, then there exists a prime number $p$ of the form $p = qn + a$ for some $n \in \mathbb{N}$. Prove that this statement also implies Dirichlet's theorem.

**Solution.** Assume that for every $a, q \in \mathbb{N}$ with $(a,q) = 1$, there is at least one prime $p$ distinct from $a$ and $p \equiv a \pmod{q}$. Let $(a,q) = 1$. Then $(a,q^n) = 1$ for every $n \in \mathbb{N}$. By the assumption, for each $n \in \mathbb{N}$, there is a prime number $p$ distinct from $a$ such that

$$p \equiv a \pmod{q^n}. \tag{7.10}$$

If $p$ is a solution of (7.10), then $p \equiv a \pmod{q}$. A prime $p$ distinct from $a$ can be a solution to (7.10) for only a finite number of $n$: if $p_1$ is a prime distinct from $a$ such that $p_1 \equiv a \pmod{q}$, then there exists $n_1 \in \mathbb{N}$ such that $q^{n_1} \parallel p_1 - a$ and we can choose a prime $p_2 \neq a$, $p_2 \neq p_1$, and $p_2 \equiv a \pmod{q^{n_1+1}}$. This implies that there are infinitely many primes $p \equiv a \pmod{q}$. □

Pollack [**299**, Chapter 2] gives the following two examples as an exercise.

**Example 7.33.** For each $n \in \mathbb{N}$, let $f(n)$ be the portion of $n!$ composed of the primes $\equiv 3 \pmod 4$, that is,

$$f(n) = \prod_{\substack{p^k \parallel n! \\ p \equiv 3 \ (\mathrm{mod}\ 4)}} p^k.$$

(i) Show that $\log f(n) = \frac{1}{2} n \log n + O(n) \sim \frac{1}{2} \log n!$.

(ii) Suppose that $n$ and $m$ are positive integers and $n! + 1 = m^8$. Prove that $f(n) \le m^2 - 1 \le (n!)^{\frac{1}{4}}$.

(iii) Deduce that the Diophantine equation $n! + 1 = m^8$ has only a finite number of solutions in positive integers $n$ and $m$.

**Solution.** The exponent of $p$ in the prime factorization of $n!$ is

$$v_p(n!) = \sum_{a=1}^{\infty} \lfloor n/p^a \rfloor .$$

Therefore $\log f(n)$ is equal to

$$\begin{aligned} &\sum_{\substack{p \le n \\ p \equiv 3 \ (\mathrm{mod}\ 4)}} v_p(n!) \log p \\ &= \sum_{\substack{p \le n \\ p \equiv 3 \ (\mathrm{mod}\ 4)}} \left\lfloor \frac{n}{p} \right\rfloor \log p + \sum_{\substack{p \le n \\ p \equiv 3 \ (\mathrm{mod}\ 4)}} \sum_{a=2}^{\infty} \left\lfloor \frac{n}{p^a} \right\rfloor \log p. \end{aligned}$$

The second sum above is less than

$$\sum_{p} \left( \sum_{a=2}^{\infty} \frac{n}{p^a} \right) \log p = n \sum_{p} \frac{\log p}{p(p-1)} \ll n.$$

The first sum is equal to

$$n \sum_{\substack{p \le n \\ p \equiv 3 \ (\mathrm{mod}\ 4)}} \frac{\log p}{p} + O\left(\sum_{p \le n} \log p\right) = \frac{1}{2} n \log n + O(n).$$

In addition, $\log n! = \sum_{m \le n} \log m = n \log n + O(n)$. So (i) is proved. For (ii), we write $n! = m^8 - 1 = (m^4+1)(m^2+1)(m^2-1)$. We observe that if $p \mid x^2+1$, then $-1$ is a quadratic residue mod $p$, which implies $p \equiv 1 \pmod 4$. So if $p \mid n!$ and $p \equiv 3 \pmod 4$, then $p \mid m^2-1$. Therefore $f(n) \mid m^2-1$, and so $f(n) \le m^2-1$. In addition,

$$m^4 + 1 \ge (m^2-1)^2 \text{ and } m^2+1 \ge m^2-1,$$

so we obtain $n! \ge (m^2-1)^4$. This proves (ii). For (iii), suppose $n!+1 = m^8$. By (ii), we have

$$\log f(n) \le \frac{1}{4} \log n!\,. \tag{7.11}$$

But by (i), $\frac{\log f(n)}{\log n!}$ converges to $\frac{1}{2}$ as $n \to \infty$. So if $n$ is large enough, then (7.11) does not hold. Therefore $n \le N$ for some $N \in \mathbb{N}$. So there are only a finite number of $n$ and $m$ satisfying $n!+1 = m^8$. ☐

**Example 7.34.** This example is to show that if $k \ge 5$ is fixed, then the Diophantine equation $n!+1 = m^k$ has only a finite number of solutions in positive integers $n$ and $m$.

(i) If $p$ and $q$ are primes, $x \in \mathbb{Z}$, and $p \mid x^q - 1$, show that $x \equiv 1 \pmod p$ or $p \equiv 1 \pmod q$.

(ii) Let $q$ be a prime and $x \ge 2$. Show that

$$\gcd\left(x-1, \frac{x^q-1}{x-1}\right) = \begin{cases} q, & \text{if } x \equiv 1 \pmod q; \\ 1, & \text{if } x \not\equiv 1 \pmod q. \end{cases}$$

In addition, if $q$ is odd and $x \equiv 1 \pmod q$, then $q \parallel \frac{x^q-1}{x-1}$.

(iii) Let $q$ be an odd prime. Show that the equation $n!+1 = m^q$ has only finitely many solutions in $n, m \in \mathbb{N}$.

(iv) Deduce that if $k$ is fixed and $k \ne 1, 2, 4$, then the equation $n!+1 = m^k$ has only a finite number of solutions in $n, m \in \mathbb{N}$.

**Solution.** Throughout this problem, let $p$ and $q$ be primes. For (i), assume that $x \in \mathbb{Z}$ and $x^q \equiv 1 \pmod p$. Then $\mathrm{ord}_p\, x \mid q$, and so $\mathrm{ord}_p\, x = 1$

or $q$. Suppose that $x \not\equiv 1 \pmod{p}$. Then $\operatorname{ord}_p x = q$. Since $(x, p) = 1$, we have $x^{p-1} \equiv 1 \pmod{p}$, by Euler's theorem. Therefore $q \mid p - 1$, as required. For (ii), Let $p$ be a prime such that $p \mid x-1$ and $p \mid \frac{x^q-1}{x-1}$. Then $x \equiv 1 \pmod{p}$ and

$$0 \equiv \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \cdots + 1 \equiv 1 + 1 + \cdots + 1 \equiv q \pmod{p}.$$

Since $q$ and $p$ are primes and $q \equiv 0 \pmod{p}$, we have $p = q$ and $x \equiv 1 \pmod{q}$. This shows that the only prime $p$ that may divide both $x - 1$ and $\frac{x^q-1}{x-1}$ is $p = q$, and in this case, we must have $x \equiv 1 \pmod{q}$. Therefore

$$\gcd\left(x - 1, \frac{x^q - 1}{x - 1}\right) = 1 \quad \text{if } x \not\equiv 1 \pmod{q}.$$

Suppose $x \equiv 1 \pmod{q}$. Then $\gcd\left(x - 1, \frac{x^q-1}{x-1}\right) = q^a$ for some $a \geq 1$. Then $x \equiv 1 \pmod{q^a}$ and

$$0 \equiv \frac{x^q - 1}{x - 1} \equiv x^{q-1} + x^{q-2} + \cdots + 1 \equiv 1 + 1 + \cdots + 1 \equiv q \pmod{q^a}.$$

Therefore $a = 1$. The remaining part of (ii) follows immediately from lifting the exponent lemma. For completeness, we also give a proof here. So suppose $q$ is odd and $x \equiv 1 \pmod{q}$. We already know that $q \mid \frac{x^q-1}{x-1}$. Suppose for a contradiction that $(x^q - 1)/(x - 1)$ is divisible by $q^2$. Then $q \parallel x - 1$, by the result on the greatest common divisor we have proved. Let $x = 1 + q\ell$, where $q \nmid \ell$. Writing

$$\frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \cdots + 1,$$

substituting $x = 1 + q\ell$, and reducing it mod $q^2$, it becomes

$$q\left(1 + \frac{q(q - 1)\ell}{2}\right),$$

which is not divisible by $q^2$, a contradiction.

For (iii), let $n! + 1 = m^q$. Then

$$n! = m^q - 1 = (m - 1)(m^{q-1} + m^{q-2} + \cdots + 1).$$

Similar to the previous example, let

$$f_1(n) = \prod_{\substack{p^k \parallel n! \\ p \equiv 1 \pmod{q}}} p^k \quad \text{and} \quad f_2(n) = \prod_{\substack{p^k \parallel n! \\ p \not\equiv 1 \pmod{q}}} p^k.$$

Then $n! = f_1(n)f_2(n)$ and $\log f_1(n)$ is equal to

$$\sum_{\substack{p\le n\\ p\equiv 1 \pmod q}} v_p(n!)\log p = \frac{n\log n}{\varphi(q)} + O(n).$$

Then $\log f_2(n)$ is equal to

$$\sum_{p\le n} v_p(n!)\log p - \log f_1(n) = \left(1 - \frac{1}{\varphi(q)}\right) n\log n + O(n). \tag{7.12}$$

Suppose $p \mid n!$ and $p \not\equiv 1 \pmod q$. Since $p \mid m^q - 1$ and $q \nmid p-1$, it follows from (i) that $p \mid m-1$. This shows that every prime in the product defining $f_2(n)$ divides $m-1$. Therefore $f_2(n) \le m-1$. In addition, $n! \ge (m-1)^q$, or equivalently, $m - 1 \le (n!)^{\frac{1}{q}}$. Thus

$$\log f_2(n) \le \frac{1}{q}\log n!\,.$$

But (7.12) implies that

$$\log f_2(n) \sim \left(1 - \frac{1}{\varphi(q)}\right)\log n!\,.$$

So if $n$ is large, then $\log f_2(n) > \frac{1}{q}\log n!$, which is not the case. So $n \le N$ for some $N \in \mathbb{N}$. This proves (iii).

For (iv), let $k \ge 5$ be fixed. If $k$ is divisible by an odd prime $q$, then the equation $n!+1 = m^k = (m^{k/q})^q$ has only a finite number of solutions in $n$ and $m$ by (iii). In the other case, $k = 2^a$ and $a \ge 3$. So we obtain from the previous example that $n!+1 = m^k = (m^{k/8})^8$ has only finitely many solutions in $n$ and $m$. This completes the proof. □

## 7.7. The Statement of the Green-Tao Theorem

In this section, we give some results on arithmetic progressions of primes and of other integer sequences. Let $a$, $q$, and $k$ be positive integers. The finite sequence $(a + qn)_{0\le n<k}$ is said to have length $k$, and it is called a $k$-term arithmetic progression with the common difference $q$. A "dual" problem of Dirichlet's theorem is the existence or nonexistence of an arithmetic progression $(a + qn)_{0\le n<k}$ consisting only of primes. For example, $(3, 5, 7)$, $(3, 7, 11)$, and $(3, 11, 19)$ are 3-term arithmetic progressions of primes, and $(7, 19, 31, 43)$ is a 4-term arithmetic progression of primes. Exercise 7.8.24 gives an example of an arithmetic progression

of primes having length 10. The famous Green-Tao theorem states that there are arbitrarily long arithmetic progressions of primes.

**Theorem 7.35.** (Green-Tao Theorem: simple version [**159**]) *If $k$ is a given positive integer, then there are distinct primes $p_1, p_2, \dots, p_k$ forming an arithmetic progression.*

Tao won the Fields Medal in 2006 for this and other various contributions. Although the proof of the Green-Tao theorem is beyond the scope of this book, the interested reader can find it in the original paper by Green and Tao [**159**], in the expository notes by Green [**158**], Kra [**231**], Conlon, Fox, and Zhao [**89**], and in the online blog of Tao. There are some extensions of the Green-Tao theorem too and we give more details about this in the notes at the end of this chapter.

Since the proof of the Green-Tao theorem is nonconstructive, it is still difficult to find a long arithmetic progression of primes. As far as we are aware, the explicit example of the longest arithmetic progression of primes known to date has length only 26.

Exercises 7.8.24 to 7.8.29 are closely related to and may follow easily from the Green-Tao theorem. This kind of question in other integer sequences is also of interest; see for example in Exercises 7.8.9, 7.8.10, 7.8.11, and 7.8.31. For another view, see Exercises 7.8.33 to 7.8.35.

## 7.8. Exercises

The exercises may be divided into two parts: those on characters (Exercises 7.8.1 to 7.8.7) and those on arithmetic progressions. To avoid triviality, all arithmetic progressions here are not the constant sequence, and for convenience, we only consider the arithmetic progressions with positive terms and positive common difference. So, throughout these exercises, we let $A(a, q)$ be the set of all $n \in \mathbb{N}$ such that $n \equiv a \pmod{q}$, where $a$ and $q$ are positive integers. We also remark that $a$ and $q$ may or may not be coprime and $A(a, q)$ may be considered as an increasing sequence $(a + qn)_{n \geq 0}$.

7.8.1 Show that if complex numbers $c_1, \dots, c_q$ are given, then

$$\sum_{\chi \bmod q} \left| \sum_{n=1}^{q} c_n \chi(n) \right|^2 = \varphi(q) \sum_{\substack{n=1 \\ (n,q)=1}}^{q} |c_n|^2 .$$

7.8.2 For each character $\chi$, let $c_\chi$ be a complex number. Show that

$$\sum_{n=1}^{q}\left|\sum_{\chi \bmod q} c_\chi \chi(n)\right|^2 = \varphi(q) \sum_{\chi \bmod q} |c_\chi|^2 .$$

7.8.3 Let $f_1, \ldots, f_m$ be the characters of a finite group $G$ of order $m$, and let $a$ be an element of $G$ of order $n$. Each number $f_r(a)$ is an $n$th root of unity. Prove that every $n$th root of unity occurs equally often among the numbers $f_1(a), f_2(a), \ldots, f_m(a)$.

7.8.4 Let $\chi$ be a nonprincipal Dirichlet character mod $q$. Prove that for all integers $a < b$, we have

$$\left|\sum_{n=a}^{b} \chi(n)\right| \leq \frac{\varphi(q)}{2}.$$

7.8.5 If $\chi$ is a real character mod $q$, then $\chi(n) = \pm 1$ or $0$ for each $n$, so the sum

$$S = \sum_{n=1}^{q} n\chi(n)$$

is an integer. This exercise shows that $12S \equiv 0 \pmod{q}$.

(i) If $(a, q) = 1$, prove that $a\chi(a)S \equiv S \pmod{q}$.

(ii) Write $q = 2^\alpha k$ where $k$ is odd. Show that there is an integer $a$ with $(a, q) = 1$ such that $a \equiv 3 \pmod{2^\alpha}$ and $a \equiv 2 \pmod{k}$. Then use (i) to deduce that $12S \equiv 0 \pmod{q}$.

7.8.6 An arithmetic function $f$ is called periodic mod $q$ if $q > 0$ and $f(m) = f(n)$ whenever $m \equiv n \pmod{q}$. The integer $q$ is called a period of $f$.

(i) If $f$ is periodic mod $q$, prove that $f$ has a smallest positive period $q_0$ and that $q_0 \mid q$.

(ii) Let $f$ be periodic and completely multiplicative, and let $q$ be the smallest positive period of $f$. Prove that $f(n) = 0$ if $(n, q) > 1$. This shows that $f$ is a Dirichlet character mod $q$.

7.8.7 Prove the following statements.

(i) Let $q \in \mathbb{N}$ and let $f$ be a Dirichlet character mod $q$. If $q$ is squarefree, prove that $q$ is the smallest period of $f$.

(ii) Give an example of a Dirichlet character modulo $q$ for which $q$ is not the smallest period of $f$.

7.8.8 Determine all right triangles with integer sides forming an arithmetic progression.

7.8.9 Show that there are arbitrarily long strings of consecutive integers each divisible by a perfect square greater than 1. (In other words, if $k \in \mathbb{N}$ is given, then we can find a positive integer $n$ such that each of $n, n+1, \ldots, n+k-1$ is divisible by a perfect square larger than 1.)

7.8.10 Show that there are arbitrarily long strings of consecutive integers that are not the sum of two squares.

7.8.11 Show that in every four consecutive integers, at least one of them is not a perfect power. (A positive integer $n$ is said to be a perfect power if $n = m^k$ for some $m, k \geq 2$.)

7.8.12 Suppose $a$ and $q$ are positive integers (not necessarily coprime). Writing $A(a,q)$ as an increasing sequence, show that $A(a,q)$ contains arbitrarily long consecutive terms that are composite numbers.

7.8.13 Let $k$ be a positive integer. Prove that there exist a prime $p$ and a strictly increasing (infinite) sequence $(a_n)_{n\geq 1}$ of positive integers such that the terms of the sequence $(p + ka_n)_{n\geq 1}$ are all primes.

7.8.14 Prove that for each positive integer $n$, there exists a prime $p > n$ such that the numbers $p \pm i$ are composite for every $i = 1, 2, \ldots, n$.

7.8.15 Let $a, q \in \mathbb{N}$ and $(a,q) = 1$. Dirichlet's theorem says that $A(a,q)$ contains infinitely many primes. This exercise gives a small extension of Dirichlet's theorem to other integer sequences related to primes.

(i) If $k \in \mathbb{N}$ is given, show that $A(a,q)$ contains infinitely many positive integers $n$ such that $\omega(n) = \Omega(n) = k$. In other words, $A(a,q)$ contains infinitely many squarefree integers having exactly $k$ prime factors.

(ii) A positive integer $n$ is called squarefull if $p^2 \mid n$ for every $p \mid n$. If $k \in \mathbb{N}$ is given, show that $A(a,q)$ contains infinitely many squarefull integers $n$ such that $\omega(n) = k$.

7.8.16 Let $a$, $q$, $k$ be positive integers, $k$ is even, and $(a,q) = 1$. Show that $A(a,q)$ contains infinitely many positive integers $n$ such that $d(n) = k$. Give an example of $a, q, k \in \mathbb{N}$ such that $(a, q) > 1$, $k$ is even, and $A(a, q)$ does not contain any $n$ such that $d(n) = k$. Give also an example where $(a, q) = 1$, $k$ is odd, and there is no $n \in A(a, q)$ with $d(n) = k$.

7.8.17 Suppose that $q$ is a prime and $1 \leq a < q$. Show that if $x$ is a primitive root of $q$, then the solutions to the equation $x^k = a + qn$ in positive integers $k$ and $n$ are given by

$$k = k_0 + (q-1)j \text{ and } n = (x^k - a)/q$$

where $j$ is any nonnegative integer and $k_0$ is the integer satisfying

$$1 \leq k_0 \leq q-1 \text{ and } x^{k_0} \equiv a \pmod{q}.$$

In addition, determine all the integers

$$a \geq b \geq 0 \text{ and } m \geq 0 \text{ such that } 2^a + 2^b = 5m.$$

7.8.18 If $1 \leq a < b \leq n$, show that

$$\gcd(n!+a, n!+b) = \gcd(a, b).$$

7.8.19 Let $n \geq 2$. Prove that each member of the set of $n$ consecutive integers

$$n!+1, n!+2, n!+3, \ldots, n!+n$$

has a prime divisor that does not divide any other member of the set.

7.8.20 Let $n$ and $k$ be positive integers. Show that there exists a set of $n$ consecutive integers such that each member of this set is divisible by $k$ distinct prime factors no one of which divides any other member of the set.

7.8.21 Let $a, d, n$ be positive integers and $n \geq 2$. Suppose that $a, a+d, \ldots, a+(n-1)d$ is an arithmetic progression of primes and $q$ is the largest prime that is less than or equal to $n$. Show that

(i) $d$ is divisible by $\prod_{p<q} p$,
(ii) if $a \neq q$, then $d$ is divisible by $\prod_{p \leq q} p$,
(iii) if $q < n$, then $d$ is divisible by $\prod_{p \leq q} p$,
(iv) $d$ is divisible by every prime $< n$.

7.8.22 Determine all arithmetic progressions $a$ mod $q$ such that $q = 10$ and $a, a+q, a+2q$ are primes. Is there such a progression with $q = 100$?

7.8.23 Suppose $a, d, r, t \in \mathbb{N}$ and $a + td, a + (t + 1)d, \ldots, a + (t + r)d$ forms an arithmetic progression of primes. If $d < 2000$, prove that $r \leq 9$.

7.8.24 Show that the arithmetic progression $(a + dk)_{0 \leq k \leq 9}$ where $a = 199$ and $d = 210$ has the following properties:
 (i) every term is a prime,
 (ii) the last term is the smallest possible among any other such arithmetic progressions.

7.8.25 Prove that there exist arbitrarily long arithmetic progressions whose terms are pairwise relatively prime. This follows easily from the Green-Tao theorem but there is a more elementary solution to this problem.

For each $m \in \mathbb{N}$ and an arithmetic function $f$, let $A(f, m)$ be the set of all $n \in \mathbb{N}$ such that $f(n) = m$. Use the Green-Tao theorem to solve Exercises 7.8.26 to 7.8.28.

7.8.26 Let $k \in \mathbb{N}$ be given. Show that there are infinitely many disjoint $k$-term arithmetic progressions of distinct primes.

7.8.27 Let $m \in \mathbb{N}$ be given. Prove the following statements.
 (i) $A(\omega, m)$ and $A(\Omega, m)$ contain arbitrarily long arithmetic progressions.
 (ii) $A(d, m)$ contains arbitrarily long arithmetic progressions if and only if $m$ is even.
 (iii) Fermat asserts that there are no four different squares of integers that form an arithmetic progression. Using this result, show that if $m$ is odd, then the length of an arithmetic progression of the numbers in $A(d, m)$ is at most 3.

7.8.28 Show that $A(\mu, 1)$ and $A(\mu, -1)$ contain arbitrarily long arithmetic progressions.

7.8.29 Let $g(n)$ be the length of the longest arithmetic progressions of primes in $[1, n]$. Show that $g(n) \ll \log n$ for all $n \geq 2$.

7.8.30 For each arithmetic function $f$ and positive integer $k$, let

$$A(f, k) = \{n \in \mathbb{N} \mid f(n) \equiv 0 \pmod{k}\}.$$

Show that if $k \in \mathbb{N}$ is given and $f = d, \varphi$, or $\sigma$ (the divisor function, the Euler function, the sum of divisors function), then $A(f, k)$ contains an infinite arithmetic progression.

7.8.31 Prove that there exist arbitrarily long arithmetic progressions whose terms are powers of positive integers with integer exponent larger than 1. Show also that if $(a_n)_{n\geq 1}$ is an infinite arithmetic progression, then $(a_n)_{n\geq 1}$ contains a term that is not a perfect power.

7.8.32 Let $a$, $b$, $c$, $d$ be nonnegative integers and $ad - bc \neq 0$. This exercise is to give an outline of Newman's theorem [**287**] which states that there are infinitely many $m, n \in \mathbb{N}$ such that $\varphi(an + b) < \varphi(cn + d)$ and $\varphi(am + b) > \varphi(cm + d)$.

(i) Let $\varepsilon > 0$ be given. Show that there exists a positive integer $N$ such that $(N, a) = 1$ and $\varphi(N)/N < \varepsilon$.

(ii) Let $N$ be any integer obtained in (i). Show that there are infinitely many positive integers $x$, $y$ such that

$$ax + b = Ny \text{ and } \varphi(ax + b) < \varepsilon(ax + b).$$

(iii) Let $x$, $y$ be any of the integers obtained in (ii) and $\delta = \gcd(cx + d, cN)$. Show that $\delta \leq |ad - bc|$ and $cx + d = \delta(A + kB)$ for some $A, B, k \in \mathbb{Z}$ with $(A, B) = 1$.

(iv) Show that we can choose $k$ in (iii) so that $k > 0$ is large and $A + Bk$ is a prime $p$. Then prove that

$$\varphi(cx + d) \geq \frac{p}{2} = \frac{cx + d}{2\delta}.$$

(v) Show that the function $x \mapsto \frac{cx+d}{ax+b}$ is monotone on $[1, \infty)$ and has a positive infimum.

(vi) Let $\alpha$ be the infimum obtained in (v) and $\varepsilon = \frac{\alpha}{2|ad-bc|}$. Prove that $(cx + d)/2\delta \geq \varepsilon(ax + b)$.

(vii) Conclude that there exists $n \in \mathbb{N}$, such that

$$\varphi(an + b) < \varphi(cn + d).$$

(viii) Deduce that there are infinitely many $m, n \in \mathbb{N}$ such that $\varphi(an + b) < \varphi(cn + d)$ and $\varphi(am + b) > \varphi(cm + d)$.

7.8.33 Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence defined by $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

(i) Determine all the 3-term arithmetic progressions of Fibonacci numbers. Deduce that $(F_n)_{n\geq 0}$ contains infinitely many 3-term arithmetic progressions.

(ii) Show that $(0, 1, 2, 3)$ is the only 4-term arithmetic progression contained in $(F_n)_{n\geq 0}$.

7.8.34 Find the arithmetic progression $A(a, q)$ that does not contain any Fibonacci number, where $a, q \in \mathbb{N}$ and $q$ is the smallest possible.

7.8.35 Find the arithmetic progression $A(a, q)$ that has the same property as in the previous exercise but with $(a, q) = 1$.

## 7.9. Notes

Exercises 7.8.1 and 7.8.2 are taken from Vaughan's lecture; see also in [**273**, p. 119]. Exercises 7.8.3 to 7.8.7 are from Apostol [**18**, pp. 155-156]. Exercises 7.8.19 and 7.8.20 are modified from Apostol [**18**, p. 128]. We slightly extend M. Cantor's result quoted in Dickson [**103**, p. 425] and Ribenboim [**342**, p. 284] and give it as Exercise 7.8.21, which then can be used to solve Exercises 7.8.22, 7.8.23, and 7.8.24. Examples 7.33 and 7.34 are adapted from Pollack [**299**, Chapter 2]. Exercise 7.8.14 appears in Pollack [**299**, Chapter 2] too and he gives credit to Sierpiński [**367**]. Example 7.30 and Exercise 7.8.31 are also from Sierpiński [**369**] and he attributes the former to Pólya and the latter to Schinzel. Nevertheless, we believe that our solution to Example 7.30 is simpler than that of Pólya or Sierpiński. Other exercises and examples are taken from various sources and they may appear in many places in the literature. Nevertheless, we also put something which may be new in Exercises 7.8.15 to 7.8.17, and 7.8.26 to 7.8.30. In particular, Exercise 7.8.29 can be obtained by an elementary method although an improved version of the Green-Tao theorem may lead to a stronger result.

Jarden observed that $\varphi(30n + 1) > \varphi(30n)$ for every positive integer $n \leq 10^4$. Newman [**287**] verified that this continues to hold for $n \leq 2 \times 10^7$. Using Dirichlet's theorem, Newman [**287**] also obtained a result which implies that contrary to what one might expect from the computational evidence, the reverse inequality $\varphi(30n + 1) < \varphi(30n)$ holds for infinitely many $n$. The smallest such $n$, which has over 1000 decimal digits, was given explicitly by Martin [**265**]. The proof of Newman's result [**287**] is outlined in Exercise 7.8.32. A second proof of his result, which avoids Dirichlet's theorem, can be found in the article by Aldaz et al. [**3**].

As mentioned in Exercise 7.8.27, Fermat asserted that the arithmetic progressions of distinct squares have length at most three. For the proof of this well-known fact, see for example in Mordell [**274**, pp. 21–22], van der Poorten [**419**], and Sierpiński [**370**, p. 75]. Pongsriiam and Subwattanachai [**326**] extended this from squares to the values of any integer-valued quadratic polynomials.

A polygonal number $P_s(n)$, or more specifically, the $n$th $s$-gonal number, is the number of points that are needed to create a regular $s$-gon with each side being of length $n-1$. It is given by

$$P_s(n) = (s/2-1)n^2 - (s/2-2)n.$$

For example, $P_3(n) = n(n+1)/2$ and $P_4(n) = n^2$ are the $n$th triangular number and the $n$th square, respectively. So $P_s(n)$ is a generalization of squares. A simple extension of Fermat's assertion is that every arithmetic progression of polygonal numbers has length at most three too, as shown by Brown, Dunn, and Harrington [**62**]. For more results in this direction, see for example in the articles by Jones and Phillips [**217**] and references therein.

If $\chi$ is a nonprincipal Dirichlet character mod $q$, let

$$S(\chi) = \max_{a,b\in\mathbb{Z}} \left| \sum_{a\le n<b} \chi(n) \right|.$$

Exercise 7.8.4 implies that $S(\chi) \le \varphi(q)/2$. A much stronger result called the Pólya–Vinogradov inequality states that $S(\chi) \ll \sqrt{q}\log q$. This inequality is close to best possible since Schur also proved that if $\chi$ is a primitive character mod $q$, then $S(\chi) \ge \sqrt{q}/2\pi$. In addition, Paley showed that there are infinitely many quadratic characters $\chi$ with $S(\chi) \gg \sqrt{q}\log\log q$ while Montgomery and Vaughan, assuming the generalized Riemann hypothesis, obtained that

$$S(\chi) \ll \sqrt{q}\log\log q \text{ for all nonprincipal characters } \chi \text{ modulo } q.$$

For more details about this, we refer the reader to Davenport [**98**, Chapter 23], and Montgomery and Vaughan [**273**, pp. 307-325]. Various proofs of the Pólya-Vinogradov inequality give explicit implied constants; see for example, in the work of Pomerance [**310**, **311**].

Exercise 7.8.34 shows that there exists an arithmetic progression whose terms are not equal to any Fibonacci number. Since $x^2 \equiv 0, 1 \pmod 4$ for all $x \in \mathbb{Z}$, the progressions $2 \pmod 4$ and $3 \pmod 4$ avoid all perfect squares. By similar reasoning, the progression $2 \pmod 3$ does not contain any triangular number (the number of the form $n(n+$

1)/2 where $n \geq 0$). Is there an arithmetic progression avoiding all the Fibonacci numbers, the Lucas numbers, triangular numbers, and squares, or in general, if a collection of sequences is given, can we determine whether there exist an arithmetic progression $a \pmod{q}$ that simultaneously avoids all terms in those sequences? We can also ask a similar question where $a$ and $q$ are required to be coprime.

Many problems in number theory involve studying the set $S$ of numbers that can be represented as a sum of elements of another set $A$ of positive integers. In some cases, $A$ is sparse but $S$ contains a lot of integers as in Waring's and Goldbach's problems. In other cases, $A$ is dense and we would like to know if nevertheless $S$ avoids a lot of integers, for instance, $S$ may avoid long arithmetic progressions or have low natural density. For each $A, B \subseteq \mathbb{N}$, we let $A \oplus B$ be the set $\{a + b \mid a \in A, b \in B \text{ and } a \neq b\}$. Chow and Long [**83**] call a set $S \subseteq \mathbb{N}$ *additively avoidable* if there exists a partition of $\mathbb{N}$ into two disjoints sets $A$ and $B$ such that $(A \oplus A) \cap S = (B \oplus B) \cap S = \emptyset$. We also say that $\{A, B\}$ avoids $S$, or $\{A, B\}$ is an additive partition avoiding $S$, $S$ is avoided by $\{A, B\}$, or $S$ generates the additive partition $\{A, B\}$. If the pair of sets $A$, $B$ is unique, then $S$ is said to be uniquely avoidable.

As mentioned in [**5**], Evans, Silverman, and Nelson independently proved that if $S$ is the set $\{F_n \mid n \geq 1\}$ of all Fibonacci numbers, then $S$ is uniquely avoidable. Alladi, Erdös, and Hoggatt [**5**, Theorem 2.2] then extended their results to a generalized Fibonacci sequence: if $F = (f_n)_{n \geq 1}$ is a linear recurrence sequence given by $f_1 = 1$, $f_2 \geq 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$, then $F$ is uniquely avoidable. They [**5**, Theorems 3.3 and 3.4] also showed that if $S = (a_n)$ is a strictly increasing sequence of positive integers which grows faster than a power of 2, that is, $a_{n+1} \geq 2a_n$, then $S$ generates infinitely many additive partitions of $\mathbb{N}$; if $S = (a_n)$ is strictly increasing but $a_n + a_m + a_\ell \equiv 0 \pmod{2}$ and $a_n + a_m > a_\ell$ for some $n < m < \ell$, then $S$ is not avoidable. There are many ways to generalize their study; see for instance, in the last section of their paper [**5**], and in the work of Hoggatt [**189**], Hoggatt and Bicknell–Johnson [**190**], Chow [**82**], Chow and Long [**83**], Krandel and Chen [**232**], and references therein.

Makowski [**257**] proved that no three consecutive integers are perfect powers. (We say that $n$ is a perfect power if $n = m^k$ for some $m, k \geq 2$.) Two consecutive integers that are perfect powers are 8 and 9. Catalan's conjecture (1844) states that these are the only pair of positive integers with this property, that is, the Diophantine equation $x^m - y^n = 1$ has a unique solution $3^2 - 2^3 = 1$ in integers $x, y, m, n \geq 2$. Then about 150 years later, Mihăilescu [**270**] gave an affirmative answer and completely solved this problem, and the result is now known as Mihăilescu's theorem.

Although Green and Tao proved the existence of arbitrarily long arithmetic progressions of primes, their proof is nonconstructive. So it is still difficult to construct a progression of primes of long length, say 100. In fact, as far as we are aware, the longest such progression known to date has length 26, discovered by Perichon in 2010, on a PlayStation 3 with software by Wroblewski and Reynolds, ported to the PlayStation 3 by Little, in a distributed PrimeGrid project. The sequence of those primes is listed as A204189 in OEIS. For minimal $k$-term arithmetic progressions of primes when $3 \leq k \leq 21$ and some prime number patterns, see the article by Granville [**155**]. Below we state the original and the polynomial versions of the Green-Tao theorem, and Szemerédi's theorem which is one of the main ingredients and inspirations in the proof of the Green-Tao theorem. We refer the reader to [**89**] and references therein for more information.

**Theorem 7.36.** (Szemerédi Theorem [**393**]) *Let A be a subset of positive integers having positive upper density, that is,*

$$\limsup_{n\to\infty} \frac{|A \cap [1, n]|}{n} > 0.$$

*Then A contains an arbitrarily long arithmetic progression.*

**Theorem 7.37.** (Green-Tao Theorem [**159**]) *Let $k \in \mathbb{N}$ be given and let A be a subset of prime numbers which have positive relative upper density, that is,*

$$\limsup_{N\to\infty} \frac{|A \cap [1, N]|}{\pi(N)} > 0.$$

*Then A contains infinitely many arithmetic progressions of length k. In particular, the increasing sequence of primes contains arbitrarily long arithmetic progressions.*

**Theorem 7.38.** (Tao and Ziegler [**398, 399**]) *Let A be a subset of primes of positive relative upper density. Then given $k \in \mathbb{N}$ and polynomials*

*$P_1, \dots, P_k \in \mathbb{Z}[m]$ with $P_1(0) = \cdots = P_k(0) = 0$, the set $A$ contains infinitely many numbers of the form*

$$n + P_1(m), \dots, n + P_k(m) \quad \text{where } n, m \in \mathbb{N}.$$

**Theorem 7.39.** (Tao and Ziegler [**400**]) *Let $d, k, r$ be positive integers and let $P_1, \dots, P_k \in \mathbb{Z}[m_1, \dots, m_r]$ be polynomials of degree at most $d$. Assume that the degree $d$ components of $P_1, \dots, P_k$ are all distinct, and suppose that for each prime $p$ there exist $n \in \mathbb{Z}$ and $\vec{m} \in \mathbb{Z}^r$ such that $n + P_1(\vec{m}), \dots, n + P_k(\vec{m})$ are all not divisible by $p$. Then there exist infinitely many natural numbers $n, m_1, \dots, m_r$ such that $n + P_1(m_1, \dots, m_r), \dots, n + P_k(m_1, \dots, m_r)$ are simultaneously prime.*

Let $g(n)$ be as in Exercise 7.8.29. Then $g(n) \ll \log n$ and the Green–Tao theorem tells us that $g(n)$ diverges to $\infty$ as $n \to \infty$. In fact, a stronger form of the Green-Tao theorem, which Green and Tao give at the end of their paper [**159**, p. 539], states that for each $k \geq 3$, there are constants $\gamma_k'$ and $N_k$ such that the number of $k$-term arithmetic progressions of primes $\leq N$ is at least $\gamma_k' N^2/(\log N)^k$. This suggests (but does not prove) that $g(N) \asymp (\log N)/(\log\log N)$. A rigorous proof is still required since $\gamma_k'$ may be very small when $k$ tends to $\infty$ with $N$. Nevertheless, the Hardy-Littlewood conjecture on prime tuples, which is still open and seems beyond our reach, implies that indeed $g(N) \asymp (\log N)/(\log\log N)$.

Consider a closely related question as follows: for each $n \in \mathbb{N}$, let

$$A(n) = \{a \in \mathbb{N} \mid 1 \leq a \leq n \text{ and } (a, n) = 1\}$$

be the least positive reduced residue system modulo $n$ and let $\ell(n)$ be the length of the longest arithmetic progressions contained in $A(n)$. Recamán (see Guy's book [**164**, Chapter B40]) asked if $\ell(n) \to \infty$ as $n \to \infty$. Stumpf [**387**] gave an affirmative answer to this question by establishing a lower bound, which diverges to $\infty$, for $\ell(n)$. Pongsriiam [**319**] completely solved this problem by giving exact formulas for $\ell(n)$ for all $n \in \mathbb{N}$. Pongsriiam [**321**] also determined all positive integers $n$ satisfying $\ell(n) = 18$ and showed that $F_{18}$, the 18th Fibonacci number, is the only Fibonacci number satisfying the equation $\ell(n) = 18$. The exact formulas for $\ell(n)$ are as follows.

**Theorem 7.40.** (Pongsriiam [**319**, Theorem 3.1]) *Suppose that $n > 1$ is squarefree and $p = P(n)$ is the largest prime factor of $n$. Then*

$$\ell(n) = \begin{cases} p-1, & \text{if } n \text{ is a prime;} \\ \frac{p+1}{2}, & \text{if } n = 2p,\ p \geq 3, \text{ and } p \equiv 3 \pmod 4; \\ p - \left\lfloor \frac{p^2}{n} \right\rfloor - 1, & \text{otherwise.} \end{cases}$$

**Theorem 7.41.** (Pongsriiam [**319**, Theorem 3.2 and Theorem 3.3]) *Suppose that $n > 1$ is not squarefree, $p = P(n)$ is the largest prime factor of $n$, and $\gamma(n) = \prod_{p|n} p$. Then*

$$\ell(n) = \max\left\{\frac{n}{\gamma(n)}, p-1\right\}.$$

We note that there may be two or more arithmetic progressions contained in $A(n)$ having maximal length. In addition, if we consider the reduced residue system different from $A(n)$, the length of longest arithmetic progressions may be more than $\ell(n)$. For example, we have $A(10) = \{1, 3, 7, 9\}$ and $\ell(10) = 2$, while $\{-3, -1, 1, 3\}$ is a set of reduced residue systems modulo 10 which contains an arithmetic progression of length $4 > \ell(10)$. In general, let $B(n)$ be a set of reduced residue systems modulo $n$ and let $\ell_B(n)$ be the length of the longest arithmetic progressions contained in $B(n)$. So if $B(10) = \{-3, -1, 1, 3\}$, then $\ell_B(10) = 4$ while $\ell(10) = 2$. From this, it is natural to consider a function $L : \mathbb{N} \to \mathbb{N}$ given by $L(n) =$

$$\max\{\ell_B(n) \mid B(n) \text{ is a set of reduced residue systems modulo } n\}.$$

Pongsriiam also obtained an exact formula for $L(n)$ in [**319**, Theorem 3.4], that is

$$L(n) = \max\left\{\frac{n}{\gamma(n)}, P(n) - 1\right\},$$

where $\gamma(n)$ and $P(n)$ are defined as in the above theorem. Since there are three problems in Chapter B39 of Guy's book [**164**] and two of them have now been completely solved, there is only one remaining: a problem on Pythagorean triples. This problem does not look difficult and the author of this book plans to solve it sometime in the future.

In general, it is also of interest to consider this kind of question in other sequences. Suppose $(a_n)$ is an integer sequence. If $a$ and $d$ are given, are there infinitely many $n \in \mathbb{N}$ such that $a_n \equiv a \pmod d$? Is the distribution of $(a_n)$ among certain residue classes modulo $d$ uniform?

Does the sequence $(a_n)$ contain arbitrarily long arithmetic progressions? For example, if for each $n \in \mathbb{N}$, $a_n$ is the $n$th prime, then the answers to these three questions are yes under some natural conditions; if $a_n = n^2$, then $a_n \equiv a \pmod{d}$ for infinitely many $n$ if and only if $a$ is a quadratic residue mod $d$, and $(a_n)$ contains arithmetic progressions of length at most three; and if $a_n$ is the $n$th Fibonacci number, then the solutions to the second and third questions are known while the first is still open for general $d$ but partial answers have been obtained; see for example in the work of Burr [**69**] Kuipers and Shiue [**235**], Niederreiter [**289**], Jacobson [**214**], Shiu and Chu [**365**], P. Bundschuh and R. Bundschuh [**66**, **67**], and Somer and Křížek [**378**, **379**].

Recall that a positive integer $n$ is called a palindrome if the decimal representation of $n$ reads the same backward as forward. For a long time, palindromes were considered only as a part of recreational mathematics, but in recent years, there has been an increasing interest in the importance of palindromes in number theory [**1**, **2**, **29**, **30**, **32**, **84**, **124**, **251**, **295**, **325**, **331**, **361**, **362**], combinatorics and computer science [**6**, **7**, **61**, **106**, **121**, **133**, **134**, **248**], and also in theoretical physics [**23**, **188**]. In particular, Harminc and Soták [**181**] showed that if $a, d \in \mathbb{N}$ and at least one of $a$, $d$ is not divisible by 10, then there are infinitely many palindromes which are congruent to $a$ mod $d$. About 17 years later, Domotorp asked on MathOverflow [**104**] whether the sequence of palindromes contains arbitrarily long arithmetic progressions. Having insight and creativity, Terry Tao [**396**] quickly gave a negative answer to this question, and from his comments, it is expected that arithmetic progressions of palindromes should have length less than $10^8$. The author of this book found this post and then showed that the length is indeed at most 10. He also made a few conjectures on this problem. For more details, see the comments at the end of his article [**323**].

**Theorem 7.42.** (Pongsriiam [**323**]) *Every arithmetic progression of palindromes has length at most* 10. *In addition,* 10 *is sharp in the sense that there are infinitely many arithmetic progressions of palindromes having length exactly* 10.

We show in Example 7.34 that if $k \neq 1, 2, 4$ is fixed, then the Diophantine equation $n! + 1 = m^k$ has only a finite number of solutions in positive integers $n$ and $m$. Erdös and Obláth [**119**] proved a more general result which implies that if $k \neq 1, 2, 4$, then $n! + 1 = m^k$ has no solution.

Pollack and Shapiro [**302**] showed that it does not have a solution either when $k = 4$. For $k = 2$, it is called the Brocard-Ramanujan equation and it is conjectured that the only solutions to $n! + 1 = m^2$ are given by $(n, m) = (4, 5)$, $(5, 11)$, and $(7, 71)$. Even the finiteness of the number of solutions is still open. Nevertheless, some special cases or variations of this equation are not too difficult to solve. For example, a Fibonacci version of this equation was first considered by Marques [**259**] and completely solved by Pongsriiam in a series of three papers [**317, 318, 322**]. A Fibonacci-like version was also solved by Szalay [**392**], Pink and Szikszai [**297**], Sahukar and Panda [**352**], and Soydan et. al [**380**].

As the reader may recall from the notes in Chapter 3, Beatty sequences can be considered as a generalization of arithmetic progressions. It is therefore natural to study the primes in Beatty sequences. There is an extensive investigation on this topic, see for example, in Banks and Shparlinski [**33**], Vaughan [**425**], Harman [**180**], and references therein. For more information on this problem, we refer the reader to the doctoral thesis by Technau [**405**].

Chapter 8

# The Riemann Zeta Function

## 8.1. Introduction

Following Riemann, we let $s$ be a complex variable and write $s = \sigma + it$ where $\sigma$ and $t$ are real. The *Riemann zeta function* is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{for all } s \in \mathbb{C} \text{ with real part } \sigma > 1.$$

Euler was the first to consider $\zeta(s)$ but only for real numbers $s > 1$ and Riemann then extended the study of $\zeta(s)$ to the complex variable $s$ with real part $\sigma > 1$. Among many other things, Riemann proved that $\zeta(s)$ is analytic on the half-plane $\sigma > 1$ and has an analytic continuation on $\mathbb{C} \setminus \{1\}$, where the point $s = 1$ is a simple pole of $\zeta(s)$ with residue 1. More precisely, the Laurent series of $\zeta(s)$ in the neighborhood of its pole $s = 1$ is

$$\zeta(s) = \frac{1}{s-1} + \gamma + \gamma_1(s-1) + \gamma_2(s-1)^2 + \cdots,$$

where $\gamma$ is Euler's constant and for $k \geq 1$,

$$\gamma_k = \frac{(-1)^k}{k!} \lim_{x\to\infty} \left( \sum_{n\leq x} \frac{(\log n)^k}{n} - \frac{(\log x)^{k+1}}{k+1} \right).$$

The series for $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is a special case of Dirichlet series, which are series of the form $\sum_{n=1}^{\infty} f(n)n^{-s}$ where $f$ is any arithmetic function.

So for example, the $L$-series defined in Chapter 7 by

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},$$

where $\chi$ is a Dirichlet character, is a Dirichlet series. We do not give a detailed study of a general theory of Dirichlet series but the interested reader can find it in Chapters 1 and 5 of Montgomery and Vaughan [**273**] or in the whole book by Hardy and Riesz [**178**]. We also refer the reader to Titchmarsh [**411**] and Ivić [**211**] for a comprehensive study of the Riemann zeta function. In this book, we focus only on the properties of Dirichlet series and the Riemann zeta function to the extent that are enough to give the proof of the prime number theorem in the next chapter.

The reader may notice that we inevitably need to assume some background from real and complex analysis but we will keep the prerequisite to a minimum. Knowledge from an undergraduate course on complex function theory is enough to understand most material in this chapter. For the reader's convenience, we also recall some definitions and well-known theorems on analytic functions which are necessary to follow the proof of all main results.

We first recall that $\sigma = \mathrm{Re}(s)$ and $t = \mathrm{Im}(s)$ denote the real and imaginary parts of $s$, respectively. In addition, for $x > 0$ and $s \in \mathbb{C}$, we define $x^s$ by $x^s = e^{s\log x}$, where $\log x$ is the real natural logarithmic of $x$. From this, we see that $x^s = e^{(\sigma+it)\log x} = x^{\sigma}e^{it\log x}$. Since $e^{i\theta} = \cos\theta + i\sin\theta$ for $\theta \in \mathbb{R}$, we have $|e^{it\log x}| = 1$ and so $|x^s| = x^{\sigma}$. Let $\Omega$ be an open subset of $\mathbb{C}$ and $f : \Omega \to \mathbb{C}$. The *derivative* of $f$ at $z_0 \in \Omega$ is given by

$$f'(z_0)=\lim_{z\to z_0}\frac{f(z)-f(z_0)}{z-z_0},$$

if the limit exists. If it does, we say that $f$ is *differentiable* at $z_0$. If $f$ is differentiable at every point in a neighborhood of $z_0$, then we say that $f$ is *holomorphic* at $z_0$. If $f$ is holomorphic at every point in an open set $U \subseteq \Omega$, we say that $f$ is holomorphic on $U$. If $f$ is holomorphic on $\Omega$, then $f$ is a holomorphic function and if $\Omega = \mathbb{C}$, then $f$ is called an *entire* function. On the other hand, $f$ is said to be *analytic* at $z_0$ if there is an open set $U \subseteq \Omega$ such that $z_0 \in U$ and $f(z) = \sum_{n=0}^{\infty} a_n(z-z_0)^n$ for all $z \in U$. If $f$ is analytic at every point in $U$, then we say that $f$ is analytic on $U$. Although the definitions of holomorphic and analytic functions are different, they are equivalent. So the words holomorphic and analytic are used interchangeably. The precise statement is as follows.

**Theorem 8.1.** *Let $\Omega$ be an open subset of $\mathbb{C}$ and $f : \Omega \to \mathbb{C}$. Then $f$ is holomorphic on $\Omega$ if and only if $f$ is analytic on $\Omega$.*

**Proof.** This can be found in [**160**, pp. 79–81] and [**383**, p. 16 and p. 49]. □

We recall the other definitions and theorems in the next section.

## 8.2. Half-Plane of Convergence

The set of points $s = \sigma + it$ with $\sigma > a$ is called a *half-plane*. We will show that for each Dirichlet series, there is a half-plane $\sigma > \sigma_c$ in which the series converges, and another half-plane $\sigma > \sigma_a$ in which it converges absolutely. The $\sigma_c$ and $\sigma_a$ are called the *abscissa of convergence* and the *abscissa of absolute convergence*, respectively. If a Dirichlet series converges throughout the plane $\mathbb{C}$, then we set $\sigma_c = -\infty$ and if it diverges everywhere, we let $\sigma_c = +\infty$. The definition for $\sigma_a = -\infty, +\infty$ is similar. We begin with the absolute convergence as follows.

**Theorem 8.2.** *Let $f : \mathbb{N} \to \mathbb{C}$ and assume that the series*

$$F(s) = \sum_{n=1}^{\infty} |f(n)n^{-s}|$$

*does not converge for all $s \in \mathbb{C}$ and does not diverge for all $s \in \mathbb{C}$. Then there exists $\sigma_a \in \mathbb{R}$ such that the series $F(s)$ converges for all $\sigma > \sigma_a$ and diverges for all $\sigma < \sigma_a$.*

**Proof.** We recall that $|n^s| = n^\sigma$. If $\sigma \geq \sigma_0$, then $|n^s| \geq n^{\sigma_0}$ and so $|f(n)n^{-s}| \leq |f(n)|n^{-\sigma_0}$. By the comparison test, if the series $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ converges at $s_0 = \sigma_0 + it_0$, then it converges for all $s \in \mathbb{C}$ with real part $\sigma \geq \sigma_0$. These observations will be used throughout this section without further reference. Let

$$A = \left\{ a \in \mathbb{R} \mid \sum_{n=1}^{\infty} |f(n)n^{-a}| \text{ converges} \right\}.$$

Since the series $F(s)$ does not diverge for all $s \in \mathbb{C}$, $A$ is not empty. In addition, $A$ has a lower bound because $F(s)$ does not converge for all $s \in \mathbb{C}$. Let $\sigma_a$ be the infimum of $A$. If $s \in \mathbb{C}$ has real part $\sigma < \sigma_a$, then $\sigma \notin A$ and therefore $F(s)$ diverges. Similarly, if $s \in \mathbb{C}$ has real part $\sigma > \sigma_a$, then $\sigma > a$ for some $a \in A$ and thus $F(s)$ converges. This completes the proof. □

We show some calculations for $\sigma_a$ in the following three examples.

**Example 8.3.** We know from calculus that $\sum_{n=1}^{\infty} n^{-p}$ converges if $p > 1$ and diverges if $p \leq 1$. So $\zeta(s)$ converges for all $s \in \mathbb{C}$ with $\sigma > 1$, and $\zeta(s)$ diverges if $s = 1$. Therefore the abscissa of absolute convergence $\sigma_a$ for $\zeta(s)$ is $\sigma_a = 1$.

**Example 8.4.** Let $\chi$ be a Dirichlet character. Since

$$|\chi(n)n^{-s}| \leq |n^{-s}|,$$

the Dirichlet $L$-series $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$ converges absolutely for all $s \in \mathbb{C}$ with $\sigma > 1$. Therefore $\sigma_a$ for $L(s,\chi)$ satisfies $\sigma_a \leq 1$. In general, if $f$ is a bounded function, then the series $\sum f(n)n^{-s}$ has $\sigma_a \leq 1$ by the comparison test.

**Example 8.5.** For each $a \in \mathbb{R}$, the series $\sum_{n=1}^{\infty} \frac{n!}{n^a}$ diverges. So the series $\sum_{n=1}^{\infty} n!\, n^{-s}$ diverges for all $s \in \mathbb{C}$. So this series has $\sigma_a = +\infty$. Similarly, $\sum_{n=1}^{\infty} \frac{1}{n!} n^{-s}$ converges for all $s \in \mathbb{C}$, so it has $\sigma_a = -\infty$.

In order to obtain the result for $\sigma_c$ analogous to Theorem 8.2, we recall that a sequence of functions $f_n : A \to \mathbb{C}$ is said to be *uniformly convergent* to the limit function $f$ on $A$ if for every $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $|f_n(x) - f(x)| < \varepsilon$ for all $n \geq N$ and $x \in A$. In addition, $f_n \to f$ *uniformly on every compact subset* of $A$ means that $f_n \to f$ uniformly on $B$ for each compact set $B \subseteq A$. We have the following results.

**Theorem 8.6.** *Let $\Omega$ be an open subset of $\mathbb{C}$, $(f_n)$ a sequence of analytic functions defined on $\Omega$, and $f : \Omega \to \mathbb{C}$. If $(f_n)$ converges uniformly to $f$ on every compact subset of $\Omega$, then $f$ is analytic on $\Omega$ and the sequence $(f_n')$ of the derivative of $f_n$ also converges uniformly to $f'$ on every compact subset of $\Omega$.*

**Theorem 8.7.** *Let $\Omega \subseteq \mathbb{C}$ be open and let $f : \Omega \to \mathbb{C}$ be an analytic function. If $f(s_n) = 0$ for infinitely many $s_n \in \Omega$ and $(s_n)$ converges to a point in $\Omega$, then $f(s) = 0$ for all $s \in \Omega$.*

Both Theorems 8.6 and 8.7 are well known. For the proof of Theorem 8.6, see for example in [**160**, pp. 88–89] or [**383**, pp. 53–54]. For Theorem 8.7, see [**383**, p. 52] or [**160**, p. 91].

The Cauchy criterion for the uniform convergence of series states that $\sum_{n=1}^{\infty} f_n(s)$ is uniformly convergent on $A$ if and only if for each $\varepsilon > 0$, there exists $K \in \mathbb{N}$ such that if $K < M < N$, then

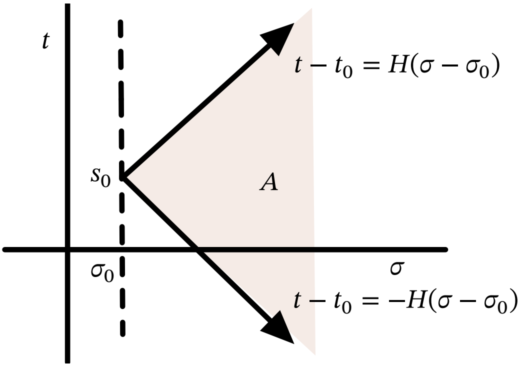
$$\left| \sum_{M<n\le N} f_n(s) \right| < \varepsilon \quad \text{for all } s \in A.$$

Applying the Cauchy criterion to $f_n(s) = f(n)n^{-s}$, we obtain the next result.

**Theorem 8.8.** *Suppose the series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converges at the point $s = s_0$. If $H > 0$ is a given constant, then the series $F(s)$ converges uniformly on $S$ where $S$ is the sector*

$$S = \{s \in \mathbb{C} \mid \ \sigma \ge \sigma_0 \textit{ and } |t - t_0| \le H(\sigma - \sigma_0)\}.$$

The picture of $S$ is shown below.


$t$
$t - t_0 = H(\sigma - \sigma_0)$
$s_0$
$A$
$\sigma_0$
$\sigma$
$t - t_0 = -H(\sigma - \sigma_0)$

**Proof.** Let $H, \varepsilon > 0$ be given and let $1 < M < N$ be integers. Since the series converges at $s = s_0$, it is natural to write the sum $\sum_{M<n\le N} f(n)n^{-s}$ as

$$\sum_{M<n\le N} f(n)n^{-s_0}n^{s_0-s} = \int_M^N t^{s_0-s} dA(t) = \int_M^N t^{s_0-s} d(A(t) - A(M)),$$

where $A(t) = \sum_{n \le t} f(n)n^{-s_0}$. Then

$$\sum_{M<n\le N} f(n)n^{-s} = \frac{A(N) - A(M)}{N^{s-s_0}} - (s_0 - s)\int_M^N (A(t) - A(M))t^{s_0-s-1}dt. \tag{8.1}$$

Since $A(t)$ converges as $t \to \infty$, we see that as $M, N \to \infty$, both $A(N) - A(M)$ and $A(t) - A(M)$ in (8.1) converge to 0. So if $M$ and $N$ are large enough and $\sigma > \sigma_0$, then

$$|A(N) - A(M)| < \varepsilon/(H+2), \quad |A(t) - A(M)| < \varepsilon/(H+2),$$

and the left-hand side of (8.1) is less than

$$\begin{aligned}&\frac{\varepsilon}{H+2} + \frac{\varepsilon}{H+2}|s - s_0|\int_M^\infty t^{\sigma_0-\sigma-1}dt \\ &= \frac{\varepsilon}{H+2} + \frac{\varepsilon|s-s_0|}{(H+2)(\sigma-\sigma_0)M^{\sigma-\sigma_0}} \le \left(1 + \frac{|s-s_0|}{\sigma-\sigma_0}\right)\frac{\varepsilon}{H+2}.\end{aligned} \tag{8.2}$$

For $s \in S$, we have

$$|s - s_0| = |(\sigma - \sigma_0) + i(t - t_0)| \le \sigma - \sigma_0 + |t - t_0| \le (H+1)(\sigma - \sigma_0).$$

Therefore if $M$ and $N$ are large and $s \in S$, then (8.2) implies that

$$\left|\sum_{M<n\le N} f(n)n^{-s}\right| < \varepsilon.$$

So by Cauchy's criterion, the series $F(s) = \sum_{n=1}^\infty f(n)n^{-s}$ converges uniformly on $S$, as desired. ☐

The result analogous to Theorem 8.2 for $\sigma_c$ is as follows.

**Theorem 8.9.** *Assume that the series $F(s) = \sum_{n=1}^\infty f(n)n^{-s}$ does not converge for all $s \in \mathbb{C}$ and does not diverge for all $s \in \mathbb{C}$. Then there exists $\sigma_c \in \mathbb{R}$ such that $F(s)$ converges for $s \in \mathbb{C}$ with $\sigma > \sigma_c$ and diverges for $\sigma < \sigma_c$.*

**Proof.** By taking $H$ in Theorem 8.8 large, we see that if $F(s)$ converges at $s = s_0$, then $F(s)$ converges for all $s$ with $\sigma > \sigma_0$. Therefore, similar to the proof of Theorem 8.2, we let

$$A = \left\{a \in \mathbb{R} \mid \sum_{n=1}^\infty f(n)n^{-a} \text{ converges}\right\},$$

and let $\sigma_c$ be the infimum of $A$. The existence of $\sigma_c$ follows from a similar argument as in Theorem 8.2. If $s \in \mathbb{C}$ has real part $\sigma$ larger than $\sigma_c$, then $\sigma > a$ for some $a \in A$ and so $\sum_{n=1}^{\infty} f(n)n^{-s}$ converges. If $s$ has real part $\sigma < \sigma_c$, then $\sigma < \frac{\sigma+\sigma_c}{2} < \sigma_c$, and so $\frac{\sigma+\sigma_c}{2} \notin A$, which implies that $\sum_{n=1}^{\infty} f(n)n^{-s}$ diverges. This completes the proof. □

Calculations for $\sigma_c$ and $\sigma_a$ are shown in the next three examples.

**Example 8.10.** Since $\sum_{n=1}^{\infty} n^{-\sigma}$ converges when $\sigma > 1$ and diverges when $\sigma \leq 1$, the series $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ converges for all $s \in \mathbb{C}$ with $\sigma > 1$ and diverges when $\sigma < 1$. Therefore $\sigma_c = 1 = \sigma_a$ for $\zeta(s)$.

**Example 8.11.** Let $F(s) = \sum_{n=1}^{\infty}(-1)^n n^{-s}$. Since $\sum_{n=1}^{\infty} |(-1)^n n^{-s}|$ converges when $\sigma > 1$ and diverges when $\sigma \leq 1$, the abscissa of absolute convergence $\sigma_a = 1$. By the alternating series test, $F(\sigma)$ converges if $\sigma > 0$, so $F(s)$ converges for all $s \in \mathbb{C}$ with $\sigma > 0$. In addition, $\lim_{n\to\infty}(-1)^n n^{-\sigma}$ does not exist if $\sigma \leq 0$, so $\sum_{n=1}^{\infty}(-1)^n n^{-\sigma}$ diverges if $\sigma \leq 0$. Therefore the abscissa of convergence $\sigma_c = 0$.

**Example 8.12.** Suppose the sum

$$\sum_{n\leq x} f(n) \quad \text{is bounded on } x \in [1, \infty).$$

Then $\sum_{n=1}^{\infty} f(n)n^{-s}$ converges for all $s \in \mathbb{C}$ with $\sigma > 0$. To see this, we recall Dirichlet's test which states that if $(a_n)$ is decreasing and converges to zero and $\sum_{n\leq x} f(n)$ is bounded on $x \in [1, \infty)$, then $\sum_{n=1}^{\infty} a_n f(n)$ converges. Therefore if $\sigma_0 > 0$ is given, then $\sum_{n=1}^{\infty} f(n)n^{-\sigma_0}$ converges which implies that $\sum_{n=1}^{\infty} f(n)n^{-s}$ converges for all $s \in \mathbb{C}$ with $\sigma > \sigma_0$. Taking $\sigma_0$ arbitrarily small, we obtain the desired result.

In particular, if $\chi(n)$ is a nonprincipal Dirichlet character mod $q$, then $\left|\sum_{n\leq x} \chi(n)\right| \leq \varphi(q)$ and so the series $\sum_{n=1}^{\infty} \chi(n)n^{-s}$ converges for $s \in \mathbb{C}$ with $\sigma > 0$. Hence this series has $\sigma_c = 0$ and $\sigma_a = 1$.

**Corollary 8.13.** *Define $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ for all $s \in \mathbb{C}$ with $\sigma > \sigma_c$. Then $F(s)$ is analytic on the half-plane $\sigma > \sigma_c$ and $F'(s)$ can be obtained by differentiating the series term by term, that is,*

$$F'(s) = -\sum_{n=1}^{\infty} f(n)(\log n)n^{-s} \quad \textit{for all } s \in \mathbb{C} \textit{ with } \sigma > \sigma_c.$$

**Proof.** If $A$ is a compact subset of the half-plane $\sigma > \sigma_c$, then by taking $s_0$ with real part $\sigma_0$ such that $\sigma_c < \sigma_0 < \min\{\mathrm{Re}(s) \mid s \in A\}$ and choosing $H$ in Theorem 8.8 large, we obtain a sector $S$ containing $A$ and $\sum_{n=1}^{\infty} f(n)n^{-s}$ converges uniformly on $A$. Therefore we obtain by Theorem 8.6 that $F(s)$ is analytic on the half-plane $\sigma > \sigma_c$ and $F'(s)$ can be obtained by differentiating $\sum_{n=1}^{\infty} f(n)n^{-s}$ term by term. ☐

**Corollary 8.14.** *The Riemann zeta function is analytic on the half-plane $\sigma > 1$. In addition, $\zeta'(s) = -\sum_{n=1}^{\infty}(\log n)n^{-s}$ for all $s \in \mathbb{C}$ with $\sigma > 1$.*

**Proof.** We know from Example 8.10 that $\zeta(s)$ has $\sigma_c = 1$. Therefore this corollary follows immediately from Corollary 8.13. ☐

The relation between $\sigma_a$ and $\sigma_c$ is as follows.

**Theorem 8.15.** *For each Dirichlet series, we have $\sigma_c \le \sigma_a \le \sigma_c + 1$.*

**Proof.** Let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ be a Dirichlet series. If the series is absolutely convergent, then it is convergent, so $\sigma_a \ge \sigma_c$. To prove the second inequality, let $\varepsilon > 0$. Since $\sum_{n=1}^{\infty} f(n)n^{-\sigma_c-\varepsilon}$ converges, the term $f(n)n^{-\sigma_c-\varepsilon}$ converges to 0 as $n \to \infty$. Then there exists a positive integer $N$ such that $|f(n)| < n^{\sigma_c+\varepsilon}$ for all $n \ge N$. Then

$$\left|f(n)n^{-\sigma_c-1-2\varepsilon}\right| < n^{-1-\varepsilon} \quad \text{for all } n \ge N.$$

Since $\sum_{n=1}^{\infty} n^{-1-\varepsilon}$ converges, we obtain by the comparison test that the series

$$\sum_{n=1}^{\infty} f(n)n^{-\sigma_c-1-2\varepsilon} \quad \text{converges absolutely.}$$

Therefore $\sigma_a \le \sigma_c + 1 + 2\varepsilon$, which holds for all $\varepsilon > 0$. Hence we obtain $\sigma_a \le \sigma_c + 1$, as required. ☐

The result analogous to Theorem 8.7 for Dirichlet series is given in the next theorem.

**Theorem 8.16.** *Let*

$$F(s) = \sum_{n=1}^{\infty} f(n)n^{-s} \quad \text{and} \quad G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$$

*be absolutely convergent series for $\sigma > \sigma_a$. Suppose $F(s_k) = G(s_k)$ for infinitely many $s_k = \sigma_k + it_k$. If $(s_k)$ converges to a point in the half-plane $\sigma > \sigma_a$ or if $\sigma_k \to +\infty$ as $k \to +\infty$, then $f(n) = g(n)$ for all $n \in \mathbb{N}$.*

**Proof.** Let $h(n) = f(n) - g(n)$ for all $n$ and let $H(s) = F(s) - G(s)$ for all $s \in \mathbb{C}$ with $\sigma > \sigma_a$. Suppose $h(n) \neq 0$ for some $n$. Let $N$ be the smallest integer such that $h(N) \neq 0$. Then we have

$$H(s) = \frac{h(N)}{N^s} + \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}, \quad \text{and so}$$

$$h(N) = N^s H(s) - N^s \sum_{n=N+1}^{\infty} h(n) n^{-s}.$$

Since $H(s_k) = 0$, the above implies that

$$h(N) = -N^{s_k} \sum_{n=N+1}^{\infty} h(n) n^{-s_k}. \tag{8.3}$$

Suppose $\sigma_k \to +\infty$ as $k \to +\infty$. So if $k$ is large enough, then there exists $c \in \mathbb{R}$ such that $\sigma_k > c > \sigma_a$ and we obtain

$$\begin{aligned} |h(N)| &\leq N^{\sigma_k} \sum_{n=N+1}^{\infty} |h(n)| n^{-\sigma_k + c} n^{-c} \\ &\leq N^{\sigma_k} (N+1)^{-\sigma_k + c} \sum_{n=N+1}^{\infty} |h(n)| n^{-c} = \left(\frac{N}{N+1}\right)^{\sigma_k} A, \end{aligned}$$

where $A$ is a constant which does not depend on $k$. By letting $k \to \infty$, we see that $(N/N+1)^{\sigma_k} A \to 0$ which implies $h(N) = 0$ contradicting the choice of $N$. Therefore $h(n) = 0$ for all $n \in \mathbb{N}$, that is,

$$f(n) = g(n) \text{ for all } n \in \mathbb{N}.$$

In the case where $s_k$ converges, we obtain by Theorem 8.7 that $H(s) = 0$ and so (8.3) holds, and the above argument is also valid. This completes the proof. □

There are many other useful and interesting results in complex function theory. We refer the interested reader to other books such as those by Greene and Krantz [**160**] or by Stein and Shakarchi [**383**].

## 8.3. Review of Infinite Products

The concept of infinite products can be defined in a similar way as infinite sums. Consider the infinite product $\prod_{n=1}^{\infty} x_n$ where $(x_n)$ is a sequence of complex numbers. For each $k \in \mathbb{N}$, let

$$P_k = \prod_{n=1}^{k} x_n = x_1 x_2 x_3 \cdots x_k \text{ be the partial product of } \prod_{n=1}^{\infty} x_n.$$

An obvious way to define the convergence of the infinite product $\prod_{n=1}^{\infty} x_n$ is to say that the sequence $(P_k)$ of partial products converges. However, for technical reasons, a slightly different definition is more useful.

**Definition 8.17.** We say that $\prod_{n=1}^{\infty} x_n$ converges if

(i) there is a positive integer $k$ such that $x_n \neq 0$ for all $n \geq k$ and
(ii) $\lim_{m\to\infty} \prod_{n=k}^{m} x_n$ exists and is not zero.

If $\prod_{n=1}^{\infty} x_n$ converges, we define its value by

$$\prod_{n=1}^{\infty} x_n = \left(\prod_{n=1}^{k-1} x_n\right)\left(\lim_{m\to\infty} \prod_{n=k}^{m} x_n\right).$$

From Definition 8.17, we see that $\prod_{n=1}^{\infty} x_n$ converges to zero if and only if there exists a positive integer $n$ such that $x_n = 0$, and there are only finitely many such $n$. For example, the infinite product $(0)(1)(1)(1)(1)(1)\cdots$ converges to zero, but the infinite products

$$(0)(1)(0)(1)(0)(1)\cdots, (1)\left(\frac{1}{2}\right)(1)\left(\frac{1}{2}\right)(1)\left(\frac{1}{2}\right)\cdots, \text{ and}$$
$$(0)(1)(2)(3)(4)(5)\cdots$$

are divergent. To be able to easily justify the convergence of the products such as

$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{4^2}\right)\left(1-\frac{1}{5^2}\right)\cdots \text{ and}$$
$$\left(1+\frac{1}{2^2}\right)\left(1+\frac{1}{3^2}\right)\left(1+\frac{1}{4^2}\right)\left(1+\frac{1}{5^2}\right)\cdots, \tag{8.4}$$

it is useful to recall some well-known results as follows.

**Theorem 8.18.** *If* $\prod_{n=1}^{\infty} x_n$ *converges, then* $(x_n)$ *converges to* 1.

**Proof.** Let $N \in \mathbb{N}$ be such that $x_n \neq 0$ for all $n \geq N$. Then for all $n > N$, $x_n = \frac{\prod_{i=N}^{n} x_i}{\prod_{i=N}^{n-1} x_i}$. Since $\prod_{i=N}^{n} x_i$ and $\prod_{i=N}^{n-1} x_i$ converges to the same nonzero limit as $n \to \infty$, we obtain $\lim_{n\to\infty} x_n = 1$ as desired. □

As a result of this theorem, it is conventional to write infinite products in the special form $\prod_{n=1}^{\infty}(1+a_n)$ and remember that $(a_n)$ converges to zero in a convergent product. In addition, we allow $a_n = -1$ only for finitely many $n$. The absolute convergence is also easy to remember.

**Definition 8.19.** Let $(a_n)$ be a sequence of complex numbers. The infinite product $\prod_{n=1}^{\infty}(1+a_n)$ is said to be absolutely convergent if $\prod_{n=1}^{\infty}(1+|a_n|)$ converges.

We next give the Cauchy criterion for infinite products, which is in a form similar to the Cauchy criterion for infinite sums. In fact, both versions can be proved in a similar way as shown in the next theorem.

**Theorem 8.20.** (Cauchy Criterion) *Assume that $a_n \neq -1$ for any $n$. Then*

$$\prod_{n=1}^{\infty}(1+a_n) \ \textit{converges if and only if} \ \lim_{m,k\to\infty}\left(\prod_{n=k}^{m}(1+a_n)\right) = 1,$$

*that is, for every $\varepsilon > 0$, there is $N \in \mathbb{N}$ such that*

$$\left|\prod_{n=k}^{m}(1+a_n) - 1\right| < \varepsilon \quad \textit{for } m \geq k \geq N.$$

**Proof.** Let $P_k = \prod_{n=1}^{k}(1+a_n)$. Assume that $\prod_{n=1}^{\infty}(1+a_n)$ converges. Then $(P_k)$ converges to a nonzero number $x$. Then there exists $N_1 \in \mathbb{N}$ such that $|P_n| > \frac{|x|}{2}$ for all $n \geq N_1$. Let $\varepsilon > 0$ be given. Since $(P_k)$ is a Cauchy sequence, there exists $N > N_1$ such that for all $m > k \geq N$, $|P_{k-1} - P_m| < \frac{\varepsilon|x|}{2}$. Then for all $m > k \geq N$, we have

$$\frac{\varepsilon|x|}{2} > |P_{k-1}|\left|\frac{P_m}{P_{k-1}} - 1\right| \geq \frac{|x|}{2}\left|\prod_{n=k}^{m}(1+a_n) - 1\right|,$$

which proves the first part. For the converse, assume that

$$\prod_{n=k}^{m}(1+a_n) = \frac{P_m}{P_{k-1}} \quad \text{converges to 1 as } m, k \to \infty \text{ and } m \geq k.$$

By letting $\varepsilon = 1$ and using the similar argument as in infinite sums, we see that $(P_k)$ is bounded. So we let $M > 0$ be such that $|P_k| \le M$ for all $k \in \mathbb{N}$. To show that $(P_k)$ converges, let $\varepsilon > 0$ be given. Then there exists $N \in \mathbb{N}$ such that

$$\left|\frac{P_m}{P_{k-1}} - 1\right| < \frac{\varepsilon}{M} \quad \text{for all } m \ge k \ge N.$$

Multiplying by $|P_{k-1}|$ on both sides, we obtain

$$|P_m - P_{k-1}| < \varepsilon \quad \text{for all } m > k \ge N.$$

This shows that $(P_k)$ is Cauchy and therefore it converges. So it remains to show that $(P_k)$ does not converge to zero. To see this, let $\varepsilon = \frac{1}{2}$, so that we obtain $M \in \mathbb{N}$ such that

$$\left|\prod_{n=k}^{m}(1 + a_n) - 1\right| < \frac{1}{2} \quad \text{for all } m > k \ge M.$$

In particular, $\prod_{n=M}^{m}(1 + a_n) > \frac{1}{2}$ for all $m \ge M$.

Let $c = \prod_{n=1}^{M-1}(1 + a_n)$. Then $c$ is a nonzero constant and

$$\left|\prod_{n=1}^{m}(1 + a_n)\right| > \frac{1}{2}|c|$$

for every $m \ge M$. This implies that

$$\lim_{k\to\infty} P_k \ge \frac{1}{2}|c|,$$

as required. □

Next we give a connection between $\prod_{n=1}^{\infty}(1+a_n)$ and $\sum_{n=1}^{\infty} a_n$. We will see that the determination of the convergence or divergence in an infinite product may be done by considering the corresponding infinite sum. We begin with a lemma.

**Lemma 8.21.** *If* $x \in [0, 1]$, *then* $1 + x \le e^x \le 1 + 2x$.

**Proof.** We define $f, g : [0, 1] \to \mathbb{R}$ by

$$f(x) = e^x - x - 1 \text{ and } g(x) = 1 + 2x - e^x$$

and then apply the usual technique in calculus to obtain the absolute extremum values of $f$ and $g$. We have $f(x) \ge f(0)$ and $g(x) \ge g(0)$ for all $x \in [0, 1]$, which lead to the desired inequality. □

**Theorem 8.22.** *Let $(a_n)$ be a sequence of complex numbers. Then $\prod_{n=1}^{\infty}(1+|a_n|)$ converges if and only if $\sum_{n=1}^{\infty}|a_n|$ converges.*

**Proof.** Applying the above lemma, we obtain

$$\prod_{n=N}^{m}(1+|a_n|) \le \exp\left(\sum_{n=N}^{m}|a_n|\right), \quad \text{and}$$

$$\exp\left(\frac{1}{2}\sum_{n=N}^{m}|a_n|\right) \le \prod_{n=N}^{m}(1+|a_n|),$$

where $N$ is a large number so that $|a_n| \le 1$ for all $n \ge N$. Then we use the monotone convergence theorem to obtain the desired result. The details are left to the reader. ☐

**Theorem 8.23.** *If $\prod_{n=1}^{\infty}(1+|a_n|)$ converges, then $\prod_{n=1}^{\infty}(1+a_n)$ converges. In other words, if $\prod_{n=1}^{\infty}(1+a_n)$ is absolutely convergent, then it is convergent.*

**Proof.** Assume that $\prod_{n=1}^{\infty}(1+|a_n|)$ converges. By Theorem 8.22, $\lim_{n\to\infty}|a_n| = 0$. So there exists $N \in \mathbb{N}$ such that $a_n \ne -1$ for all $n \ge N$. So the first condition for the convergence of $\prod_{n=1}^{\infty}(1+a_n)$ is checked. Next, let $P_k = \prod_{n=N}^{k}(1+a_n)$ and $Q_k = \prod_{n=N}^{k}(1+|a_n|)$ for every $k \ge N$. We first observe that $P_k = 1+f$, where $f$ is a polynomial in $a_N, a_{N+1}, \dots, a_k$ and $Q_k = 1+f^*$, where each term of $f^*$ is the absolute value of the corresponding term of $f$. Therefore

$$|P_k - 1| = |f| \le f^* = Q_k - 1 \text{ for every } k \ge N.$$

In general,

$$\left|\prod_{n}(1+a_n) - 1\right| \le \prod_{n}(1+|a_n|) - 1 \tag{8.5}$$

for any product taken over a finite number of $n$. Now for $m > k \ge N$, we obtain by (8.5) that $\left|\frac{P_m}{P_k} - 1\right| \le \frac{Q_m}{Q_k} - 1$ and therefore

$$\begin{aligned}|P_m - P_k| = |P_k|\left|\frac{P_m}{P_k} - 1\right| &\le |P_k|\left(\frac{Q_m}{Q_k} - 1\right)\\ &\le Q_k\left(\frac{Q_m}{Q_k} - 1\right) \le |Q_m - Q_k|.\end{aligned}$$

Since $(Q_k)_{k\geq N}$ is convergent, $(P_k)_{k\geq N}$ is also convergent. It remains to show that $\lim_{k\to\infty} P_k \neq 0$. By the Cauchy criterion, there exist integers $M > N > 0$ such that

$$\prod_{n=m}^{k}(1+|a_n|)-1<\frac{1}{2}$$

for every $k > m \geq M$. So by (8.5), we obtain that

$$\left|\prod_{n=m}^{k}(1+a_n)-1\right|<\frac{1}{2}\quad \text{for every } k>m\geq M.$$

Therefore $\prod_{n=m}^{k}(1+a_n)>\frac{1}{2}$ for every $k > m \geq M$. In particular,

$$\prod_{n=M+1}^{k}(1+a_n)>\frac{1}{2}\quad \text{for each } k>M+1.$$

Then

$$\begin{aligned}\lim_{k\to\infty}|P_k| &= \lim_{k\to\infty}\left|\prod_{n=N}^{k}(1+a_n)\right| = \lim_{k\to\infty}\left|\prod_{n=N}^{M}(1+a_n)\prod_{n=M+1}^{k}(1+a_n)\right| \\ &= \left|\prod_{n=N}^{M}(1+a_n)\right| \lim_{k\to\infty}\left|\prod_{n=M+1}^{k}(1+a_n)\right| \\ &\geq \frac{1}{2}\left|\prod_{n=N}^{M}(1+a_n)\right|>0.\end{aligned}$$

This completes the proof. ☐

**Corollary 8.24.** *If the series $\sum_{n=1}^{\infty}|a_n|$ converges, then the product $\prod_{n=1}^{\infty}(1+a_n)$ converges.*

**Proof.** This follows from Theorems 8.22 and 8.23. ☐

By Corollary 8.24, it is now easy to see that the infinite products in (8.4) are convergent.

## 8.4. Euler Product Formula

We are now ready to give the proof of the Euler product formula which connects an infinite sum of a multiplicative function with an infinite product. Intuitively, the reason behind this formula is the fundamental theorem of arithmetic and an argument similar to that given in the proof of Theorem 2.22 in Chapter 2. Nevertheless, since there is a problem on the convergence or divergence of an infinite product, a rigorous and careful proof is required.

**Theorem 8.25.** (Euler Product Formula) *Let $f$ be a multiplicative function. Assume that $\sum_{n=1}^{\infty} f(n)$ converges absolutely. Then*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} (1 + f(p) + f(p^2) + \cdots),$$

*where the product is taken over all prime numbers and is absolutely convergent. If, in addition, $f$ is completely multiplicative, then*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} (1 - f(p))^{-1}.$$

**Proof.** We recall from Theorems 8.22 and 8.23 that

$$\prod_{n=1}^{\infty} (1 + a_n) \quad \text{absolutely converges if} \sum |a_n| \text{ converges.}$$

So we consider

$$\sum_{p} |f(p) + f(p^2) + \cdots| \le \sum_{p} |f(p)| + \sum_{p} |f(p^2)| + \cdots \le \sum_{n=2}^{\infty} |f(n)|.$$

Therefore the product $\prod_p (1 + f(p) + f(p^2) + \cdots)$ absolutely converges. Next, let

$$P(x) = \prod_{p \le x} (1 + f(p) + f(p^2) + \cdots).$$

When $x$ is fixed, the number of factors of $P(x)$ is finite and each is an absolutely convergent series since $\sum |f(n)|$ converges. Therefore, by Cauchy's theorem on multiplications of series, we can multiply the terms and arrange them in any order we like which will be absolutely convergent. By the multiplicative property of $f$, a typical term of the series is

$$f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}) = f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}),$$

where $2 = p_1 < p_2 < \cdots < p_k \le x$ are the primes less than or equal to $x$ and $a_1, a_2, \ldots, a_k$ are nonnegative integers. Since every $n > 1$ can be expressed uniquely as a product of prime numbers, we obtain

$$P(x) = \sum_{n \in A} f(n)$$

where $A$ is the set of all positive integers having all prime factors less than or equal to $x$. Then

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n\in B} f(n),$$

where $B$ is the set of all positive integers having a prime factor larger than $x$. Therefore

$$\left|\sum_{n=1}^{\infty} f(n) - P(x)\right| \le \sum_{n\in B} |f(n)| \le \sum_{n>x} |f(n)| = \sum_{n=1}^{\infty} |f(n)| - \sum_{n\le x} |f(n)|,$$

which converges to 0 as $x \to \infty$. Hence $P(x)$ converges to $\sum_{n=1}^{\infty} f(n)$ as $x \to \infty$. If $f$ is completely multiplicative, then $f(p^n) = f(p)^n$ for every $n$ and the product is equal to

$$\prod_p (1 + f(p) + (f(p))^2 + (f(p))^3 + \cdots) = \prod_p (1 - f(p))^{-1}.$$

We remark that we already obtained the convergence of the geometric series $1 + f(p) + (f(p))^2 + (f(p))^3 + \cdots$. So $|f(p)| < 1$ and the formula $\sum_{n=0}^{\infty} (f(p))^n = (1 - f(p))^{-1}$ which we apply in the above calculation is valid. ☐

Applying the Euler product formula to absolutely convergent Dirichlet series, we obtain the following result.

**Theorem 8.26.** *Assume that $\sum_{n=1}^{\infty} f(n)n^{-s}$ converges absolutely for $\sigma > \sigma_a$. If $f$ is multiplicative and $s \in \mathbb{C}$ has real part $\sigma > \sigma_a$, then*

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_p \left(1 + f(p)p^{-s} + f(p^2)p^{-2s} + \cdots\right).$$

*In addition, if $f$ is completely multiplicative, then*

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_p (1 - f(p)p^{-s})^{-1} \quad \text{for } \sigma > \sigma_a.$$

*Furthermore, each product is absolutely convergent for $\sigma > \sigma_a$.*

**Proof.** This follows immediately from Theorem 8.25. ☐

Substituting $f(n) = 1, \mu(n), \varphi(n), d(n), \sigma(n), \lambda(n), \chi(n)$ in Theorem 8.26, we obtain the following formulas.

**Corollary 8.27.** *For $s \in \mathbb{C}$ with real part $\sigma$, the following formulas hold.*

(i) $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ *if* $\sigma > 1$.

(ii) $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p (1 - p^{-s}) = \frac{1}{\zeta(s)}$ *if* $\sigma > 1$.

(iii) $\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \prod_p (1 + p^{-s})^{-1} = \frac{\zeta(2s)}{\zeta(s)}$ *if* $\sigma > 1$.

(iv) $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1 - \chi(p)p^{-s})^{-1}$ *if* $\sigma > 1$.

*Furthermore, each product in* (i) *to* (iv) *is absolutely convergent.*

**Proof.** We recall that $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ converges absolutely for $\sigma > 1$. So we can apply Theorem 8.26 to $\zeta(s)$ and obtain (i). Since $|\mu(n)n^{-s}| \le n^{-\sigma}$ for all $n \in \mathbb{N}$ and $\sum_{n=1}^{\infty} n^{-\sigma}$ converges if $\sigma > 1$, we see that the series in (ii) converges absolutely for $\sigma > 1$. Similarly, since $|\lambda(n)| \le 1$ and $|\chi(n)| \le 1$ for all $n \in \mathbb{N}$, the series in (iii) and (iv) are absolutely convergent for $\sigma > 1$. Since the functions $\lambda$ and $\chi$ are completely multiplicative, we obtain (ii), (iii), and (iv) by Theorem 8.26. This completes the proof. ☐

Next we give another result that helps in finding Euler products of Dirichlet series.

**Theorem 8.28.** *Assume that the Dirichlet series* $\sum_{n=1}^{\infty} f(n)n^{-s}$ *and* $\sum_{n=1}^{\infty} g(n)n^{-s}$ *converge absolutely for* $\sigma > a$ *and* $\sigma > b$*, respectively. Then for* $\sigma > \max\{a, b\}$*, we have*

$$\left(\sum_{n=1}^{\infty} f(n)n^{-s}\right)\left(\sum_{n=1}^{\infty} g(n)n^{-s}\right) = \sum_{n=1}^{\infty} h(n)n^{-s},$$

*where* $h = f * g$*, the Dirichlet product of* $f$ *and* $g$*:*

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

**Proof.** Let $\sigma > \max\{a, b\}$. Since both $\sum f(n)n^{-s}$ and $\sum g(n)n^{-s}$ converge absolutely, we can multiply these series and rearrange the terms as we like. We have

$$\left(\sum_{n=1}^{\infty} f(n)n^{-s}\right)\left(\sum_{m=1}^{\infty} g(m)m^{-s}\right) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} f(n)g(m)(nm)^{-s}.$$

Collecting the terms that have $nm = k$, the above becomes

$$\sum_{k=1}^{\infty}\left(\sum_{nm=k} f(n)g(m)\right)k^{-s} = \sum_{k=1}^{\infty} h(k)k^{-s},$$

where $h(k) = \sum_{nm=k} f(n)g(m) = (f * g)(k)$. This completes the proof. ☐

**Corollary 8.29.** *For $s \in \mathbb{C}$ with real part $\sigma$, we have*

(i) $\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} = \prod_p (1-p^{-s})\left(1-p^{1-s}\right)^{-1}$ *if* $\sigma > 2$,

(ii) $\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta^2(s) = \prod_p (1-p^{-s})^{-2}$ *if* $\sigma > 1$,

(iii) $\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta(s-1)\zeta(s) = \prod_p \left(1-p^{1-s}\right)^{-1} (1-p^{-s})^{-1}$ *if* $\sigma > 2$.

**Proof.** Since the divisor function $d = 1 * 1$ and $\sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$, we obtain by Theorem 8.28 and Corollary 8.27 that

$$\sum_{n=1}^{\infty} d(n)n^{-s} = \zeta(s)\zeta(s) = \zeta^2(s) = \prod_p (1-p^{-s})^{-2} \quad \text{for } \sigma > 1.$$

Since $|\varphi(n)| \le n$, then $|\varphi(n)n^{-s}| \le n^{-\sigma+1}$. Since $\sum_{n=1}^{\infty} n^{-\sigma+1}$ converges if $\sigma > 2$, the series $\sum_{n=1}^{\infty} \varphi(n)n^{-s}$ converges absolutely for $s \in \mathbb{C}$ with $\sigma > 2$. In addition, $1 * \varphi = N$. Therefore we obtain by Theorem 8.28 that

$$\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}\right) = \left(\sum_{n=1}^{\infty} \frac{n}{n^s}\right) = \zeta(s-1) \quad \text{for } \sigma > 2,$$

which implies (ii). Similarly, since $\sigma = N * 1$, the formula (iii) follows from Theorem 8.28 and Corollary 8.27. This completes the proof. ☐

**Corollary 8.30.** *For $s \in \mathbb{C}$ with $\sigma > 1$, we have*

(i) $\zeta(s) \ne 0$,

(ii) $\log \zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s}$,

(iii) $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n)n^{-s}$.

*Here the branch of* $\log \zeta(s)$ *is taken so that it is real on the real axis.*

**Proof.** Let $\sigma > 1$. By Corollary 8.27, we know that

$$\zeta(s) = \prod_p (1-p^{-s})^{-1}$$

and the product is absolutely convergent and has no zero factors. So $\zeta(s) \ne 0$. Let $s \in \mathbb{R}$ and $s > 1$. Taking the logarithm on both sides of the

Euler product for $\zeta(s)$, we obtain that

$$\log\zeta(s) = \sum_p \log(1-p^{-s})^{-1} = \sum_p \sum_{k=1}^{\infty} \frac{p^{-ks}}{k} = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s}.$$

We note that it is not true in general that $\log(s_1 s_2) = \log s_1 + \log s_2$ for $s_1, s_2 \in \mathbb{C}$ but the above calculation is valid since $s \in \mathbb{R}$. So (ii) holds for $s \in \mathbb{R}$ and $s > 1$. In addition, $|\Lambda(n)| \le \log n$ for all $n \in \mathbb{N}$. So the right-hand side of (ii) is also analytic on the half-plane $\sigma > 1$. Since both sides of (ii) are analytic on the half-plane $\sigma > 1$ and they agree on $[1, \infty)$, we conclude from Theorem 8.7 that they agree everywhere on this half-plane. This proves (ii). For (iii), we recall that $\Lambda * 1 = \log$. So we obtain by Theorem 8.28 that

$$\left(\sum_{n=1}^{\infty} \Lambda(n) n^{-s}\right)\zeta(s) = \sum_{n=1}^{\infty} (\log n) n^{-s} = -\zeta'(s),$$

which implies (iii). Alternatively, by differentiating both sides of (ii), we see that

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \sum_{k=1}^{\infty} (\log p) p^{-ks} = -\sum_{n=1}^{\infty} \Lambda(n) n^{-s}.$$ ☐

## 8.5. Analytic Continuation

In this section, we give an analytic continuation of $\zeta(s)$ beyond the half-plane in which it is initially defined. We first prove the following result.

**Theorem 8.31.** *For $s \in \mathbb{C}$ with $\sigma > 1$, we have*

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt.$$

**Proof.** By partial summation or by using Euler's summation formula, we obtain

$$\begin{aligned}\sum_{n \le x} n^{-s} &= 1 + \int_1^x t^{-s} d\lfloor t \rfloor = 1 + \int_1^x t^{-s} dt - \int_1^x t^{-s} d\{t\} \\ &= \frac{x^{1-s}}{1-s} + \frac{s}{s-1} - \frac{\{x\}}{x^s} - s\int_1^x \frac{\{t\}}{t^{s+1}} dt.\end{aligned}$$

Taking $x \to \infty$, we obtain the desired result. ☐

**Theorem 8.32.** *The formula in Theorem* 8.31 *gives an analytic continuation of* $\zeta(s)$ *to the half-plane* $\sigma > 0$ *with the simple pole at* $s = 1$ *with residue* 1.

**Proof.** Since the function $s \mapsto \frac{s}{s-1} = \frac{1}{s-1} + 1$ is analytic at every point on $\sigma > 0$ except a simple pole at $s = 1$ with residue 1, it is enough to show that the function $f$ defined by $f(s) = \int_1^\infty \frac{\{t\}}{t^{s+1}} dt$ is analytic on $\sigma > 0$. For each $m \in \mathbb{N}$, let $f_m$ be defined by

$$f_m(s) = \int_1^m \frac{\{t\}}{t^{s+1}} dt \quad \text{for } s \in \mathbb{C} \text{ with } \sigma > 0.$$

Since the integrand is an analytic function of $s$, it is not difficult to see that $f_m$ is analytic on the half-plane $\sigma > 0$. Alternatively, we can write $f_m(s)$ as a power series as follows. We observe that

$$f_m(s) = \int_1^m \{t\} e^{-(s+1)\log t} dt = \int_1^m \sum_{n=0}^\infty \frac{\{t\}(-\log t)^n (s+1)^n}{n!} dt,$$

$$\begin{aligned} \sum_{n=0}^\infty \left| \frac{\{t\}(-\log t)^n (s+1)^n}{n!} \right| &\le \sum_{n=0}^\infty \frac{(|\log t|(|s|+1))^n}{n!} \\ &= e^{|\log t|(|s|+1)}, \quad \text{and} \end{aligned}$$

$$\int_1^m \sum_{n=0}^\infty \left| \frac{\{t\}(-\log t)^n (s+1)^n}{n!} \right| dt \le \int_1^m t^{|s|+1} dt < \infty.$$

By Fubini's theorem, we can change the order of integration and obtain

$$f_m(s) = \sum_{n=0}^\infty \frac{(s+1)^n}{n!} \int_1^m \{t\}(-\log t)^n dt,$$

which is just a power series of $s$. To see that $f_m \to f$ uniformly on every compact subset of the half-plane $\sigma > 0$, we consider on the half-plane $\sigma \ge \delta$ and obtain

$$|f_m(s) - f(s)| \le \int_m^\infty \frac{1}{t^{\sigma+1}} dt \ll \frac{1}{\sigma m^\sigma} \le \frac{1}{\delta m^\delta}.$$

So if $\varepsilon, \delta > 0$ are given, we can choose $M > 0$ depending on $\varepsilon$ and $\delta$ but not on $s$ (for example, $M = (\delta\varepsilon)^{-\frac{1}{\delta}}$) such that $|f_m(s) - f(s)| < \varepsilon$ for every $m > M$ and for every $s \in \mathbb{C}$ with $\sigma \ge \delta$. This completes the proof. ☐

It is possible to extend Theorems 8.31 and 8.32 and obtain an analytic continuation for $\zeta(s)$ on $\mathbb{C} \setminus \{1\}$ but it is not necessary for the proof of the prime number theorem. So we only give an outline of the proof as follows. Theorem 8.31 can be written in another form as

$$\zeta(s) = \frac{s}{s-1} - \frac{1}{2} - \int_1^\infty \frac{((x))}{x^{s+1}}dx,$$

where $((x))$ is the saw tooth function defined by $((x)) = \{x\} - \frac{1}{2}$ for all $x \in \mathbb{R}$. The Bernoulli polynomials defined in Chapter 4 are generalizations of the saw tooth function and can be used to extend Theorems 8.31 and 8.32. By writing

$$\zeta(s) = \sum_{n \le N} n^{-s} + \sum_{n > N} n^{-s}$$

and applying the Euler-Maclaurin summation formula to the second sum, we see that

$$\begin{aligned}\zeta(s) = \sum_{n \le N} n^{-s} + \frac{N^{1-s}}{s-1} + N^{-s} \sum_{k=1}^{m} \binom{s+k-2}{k-1} B_k N^{-k+1}/k \\ - \binom{s+m-1}{m} \int_N^\infty B_m(\{x\}) x^{-s-m} dx.\end{aligned}$$

The above is valid for $s \in \mathbb{C}$ with $\sigma > 1$ but the right-hand side is analytic for $s \in \mathbb{C}$ with $\sigma > 1 - m$. Therefore this gives an analytic continuation for $\zeta(s)$ on the half-plane $\sigma > 1 - m$. Since $m$ is an arbitrary positive integer, we obtain an analytic continuation for $\zeta(s)$ on $\mathbb{C} \setminus \{1\}$. A functional equation for $\zeta(s)$ and an alternative way to obtain an analytic continuation for $\zeta(s)$ is also outlined in the notes in Section 8.8.

## 8.6. Zero Free Regions

We know from Corollary 8.30 that $\zeta(s) \neq 0$ on the half-plane $\sigma > 1$. In other words, the half-plane $\sigma > 1$ is a *zero free region* for $\zeta(s)$. Extending this region to the boundary $\sigma = 1$ is not trivial. At the heart of the proof of the prime number theorem that we give in the next chapter lies the fact that

$$\zeta(s) \neq 0 \quad \text{on the line } \sigma = 1. \tag{8.6}$$

For zero free regions larger than (8.6) see the notes in Section 8.8. To prove (8.6), we need the following lemmas.

**Lemma 8.33.** *If* $\theta \in \mathbb{R}$, *then* $3 + 4\cos\theta + \cos 2\theta \geq 0$.

**Proof.** We have $\cos^2\theta = (1+\cos 2\theta)/2$. So this lemma follows from the observation that $3+4\cos\theta+\cos 2\theta = 2(1+\cos\theta)^2$. ☐

**Lemma 8.34.** *If* $\sigma > 1$ *and* $t \in \mathbb{R}$, *then*

$$\log\left|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)\right| \geq 0.$$

**Proof.** Let $\sigma > 1$, $t \in \mathbb{R}$, and $s = \sigma + it$. We recall that for any nonzero complex number $z$, we have $\operatorname{Re}(\log z) = \log|z|$. Therefore $\log\left|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)\right|$ is equal to

$$\begin{aligned} &3\log|\zeta(\sigma)| + 4\log|\zeta(s)| + \log|\zeta(\sigma+2it)| \\ &= 3\operatorname{Re}(\log\zeta(\sigma)) + 4\operatorname{Re}(\log\zeta(s)) + \operatorname{Re}(\log\zeta(\sigma+2it)). \end{aligned} \tag{8.7}$$

In addition, $\operatorname{Re}(n^{-s}) = n^{-\sigma}\cos(t\log n)$. For each $n \in \mathbb{N}$, let $\theta_n = t\log n$. Then by Corollary 8.30, we obtain

$$\begin{aligned} \operatorname{Re}(\log\zeta(s)) &= \sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n}\operatorname{Re}(n^{-s}) = \sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n}n^{-\sigma}\cos\theta_n, \\ \operatorname{Re}(\log\zeta(\sigma)) &= \sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n}n^{-\sigma}, \quad \text{and} \\ \operatorname{Re}(\zeta(\sigma+2it)) &= \sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n}n^{-\sigma}\cos 2\theta_n. \end{aligned}$$

Hence (8.7) is

$$\sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n}n^{-\sigma}(3+4\cos\theta_n+\cos 2\theta_n) \geq 0,$$

by Lemma 8.33. This completes the proof. ☐

**Theorem 8.35.** $\zeta(s) \neq 0$ *for* $s \in \mathbb{C}$ *with* $\sigma = 1$.

**Proof.** Suppose for a contradiction that $\zeta(1+it) = 0$ for some $t \in \mathbb{R}$. By Theorem 8.32, $\zeta(s)$ is analytic at every point on the line $\sigma = 1$ except a simple pole at $s = 1$. Therefore $\zeta^3(\sigma)$ has a pole of order 3 at $\sigma = 1$ and $\zeta^4(\sigma+it)$ has a zero of order at least 4 at $\sigma = 1$, and thus $\lim_{\sigma\to 1^+}\zeta^4(\sigma+it)\zeta^3(\sigma) = 0$. In addition,

$$\lim_{\sigma\to 1^+}\zeta(\sigma+2it) = \zeta(1+2it).$$

Hence

$$\lim_{\sigma\to 1^+}\zeta^4(\sigma+it)\zeta^3(\sigma)\zeta(\sigma+2it) = 0.$$

But by Lemma 8.34, $|\zeta^4(\sigma+it)\zeta^3(\sigma)\zeta(\sigma+2it)| \geq 1$ for all $\sigma > 1$, so the limit as $\sigma \to 1^+$ cannot be zero, a contradiction. This completes the proof. $\square$

## 8.7. Exercises

Exercises 8.7.7 to 8.7.9 are the continuation of Exercises 4.8.15 and 4.8.16. They are an outline to obtain the exponential generating functions for $B_n(x)$ and $B_n$ from their inductive definitions. So combining Exercises 4.8.13, 8.7.8, and 8.7.9, we see that the two definitions are equivalent. Other exercises are from Apostol [**18**, Chapter 12].

8.7.1 Apply Weierstrass's M-test to show that the series $\sum_{n=1}^{\infty} n^{-s}$ converges uniformly on the half-plane $\sigma \geq 1+\delta$ for any $\delta > 0$. Then use this to give another proof of Corollary 8.14.

8.7.2 Suppose $\sum_{n=1}^{\infty} f(n)n^{-s}$ converges at $s = s_0$. Show that the series converges uniformly on every compact subset of the half-plane $\sigma > \sigma_0$.

8.7.3 Let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ for $s \in \mathbb{C}$ with $\sigma > \sigma_a$. Show that

$$\lim_{\sigma\to+\infty} F(\sigma+it) = f(1) \text{ uniformly for } t \in \mathbb{R},$$

that is, for each $\varepsilon > 0$, there exists $\sigma_0 \in \mathbb{R}$ such that if $\sigma > \sigma_0$, then $|F(\sigma+it) - f(1)| < \varepsilon$ for all $t \in \mathbb{R}$.

8.7.4 Let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ and $F(s) \neq 0$ for some $s \in \mathbb{C}$ with $\sigma > \sigma_a$. Then there exists $c \in \mathbb{R}$ such that $c \geq \sigma_a$ and $F(s) \neq 0$ for any $s$ in the half-plane $\sigma > c$.

8.7.5 Let $g = f^{-1}$ be the Dirichlet inverse of $f$. Show that in the half-plane where both series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ and $G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$ are absolutely convergent, we have $F(s) \neq 0$ and $G(s) = 1/F(s)$.

8.7.6 Let $f$ be completely multiplicative and $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converges absolutely for $\sigma > \sigma_a$. Show that

$$\sum_{n=1}^{\infty} \mu(n)f(n)n^{-s}$$

converges absolutely and is equal to $1/F(s)$ for $\sigma > \sigma_a$.

8.7.7 Show that

(i) $B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$ for every $n \geq 0$,

(ii) $B_n = \sum_{k=0}^{n} \binom{n}{k} B_k$ for every $n \geq 2$.

8.7.8 Show that

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n z^n}{n!} \quad (|z| < 2\pi).$$

8.7.9 Show that

$$\frac{ze^{xz}}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n(x) z^n}{n!} \quad (|z| < 2\pi).$$

8.7.10 Prove that the Bernoulli polynomials satisfy the following formulas:

(i) (Addition Formula) $B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x) y^{n-k}$,

(ii) (Multiplication Formula)

$$B_n(mx) = m^{n-1} \sum_{k=0}^{m-1} B_n\left(x + \frac{k}{m}\right).$$

8.7.11 Let $r \in \mathbb{N}$. Show that

$$\sum_{k=0}^{r} \frac{2^{2k} B_{2k}}{(2k)!\,(2r+1-2k)!} = \frac{1}{(2r)!}.$$

8.7.12 Let $B_n$ be the $n$th Bernoulli number. Show that if $n \geq 1$, we have

$$B_{2n} = I_n - \sum_{p-1 | 2n} \frac{1}{p},$$

where $I_n$ is an integer and the sum is over all primes $p$ such that $p-1$ divides $2n$. These formulas were discovered in 1840 by von Staudt and Clausen (independently). This exercise outlines a proof due to Lucas. Prove the following statements.

(i) For $n \geq 1$, $B_n = \sum_{k=0}^{n} \frac{1}{k+1} \sum_{r=0}^{k} (-1)^r \binom{k}{r} r^n$.

(ii) For $n \geq 1$, $B_n = \sum_{k=0}^{n} \frac{k!}{k+1} c(n,k)$, where $c(n,k)$ is an integer.

(iii) If $k > 3$ and $k+1$ is composite, then $k!$ is divisible by $k+1$.

(iv) If $n \in \mathbb{N}$ and $p$ is prime, then

$$\sum_{r=0}^{p-1}(-1)^r\binom{p-1}{r}r^n \equiv \begin{cases} -1 \pmod{p}, & \text{if } p-1 \mid n, n > 0; \\ 0 \pmod{p}, & \text{if } p-1 \nmid n. \end{cases}$$

(v) Prove the von Staudt-Clausen theorem.

## 8.8. Notes

In this section, we say something more on the zero-free region for $\zeta(s)$ and another way to obtain an analytic continuation of $\zeta(s)$ on $\mathbb{C} \setminus \{1\}$. We also give the statement of the famous Riemann hypothesis and a few recent results on this problem.

Riemann obtained an analytic continuation for $\zeta(s)$ on $\mathbb{C} \setminus \{1\}$ from his functional equation, which is shown in (8.9) and (8.10). We first recall that the gamma function $\Gamma$, the theta function $\vartheta$, and the xi function $\xi$ are defined by

$$\Gamma(s) = \int_0^\infty e^{-x}x^{s-1}dx \quad \text{for } s \in \mathbb{C} \text{ with } \sigma > 1,$$

$$\vartheta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t} \quad \text{for } t > 0,$$

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) \quad \text{for } s \in \mathbb{C} \text{ with } \sigma > 1. \tag{8.8}$$

It can be shown that $\Gamma$ is analytic on the half-plane $\sigma > 1$ and has an analytic continuation to a meromorphic function on $\mathbb{C}$ with the simple poles at the integers $s = -n$ where $n \geq 0$. The residue at $s = -n$ is $(-1)^n/n!$. In addition,

$$\sqrt{t}\vartheta(t) = \vartheta\left(\frac{1}{t}\right).$$

By using some properties of $\Gamma$ and $\vartheta$, one can prove that the function $\xi$ is analytic on $\sigma > 1$ and has an analytic continuation on $\mathbb{C}$ except simple poles at $s = 0$ and $s = 1$. Moreover, $\xi(s) = \xi(1-s)$ for all $s \in \mathbb{C}\setminus\{0, 1\}$. To remove the singularities at $s = 0$ and $s = 1$, we can adjust the definition of $\xi$ in (8.8) and define it instead by

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s). \tag{8.9}$$

Then $\xi$ is entire, $\xi(s) = \xi(1-s)$ for all $s \in \mathbb{C}$, and

$$\zeta(s) = \frac{2\xi(s)\pi^{s/2}}{s(s-1)\Gamma(s/2)} \tag{8.10}$$

which gives an analytic continuation for $\zeta(s)$ onto $\mathbb{C} \setminus \{1\}$ with a simple pole at $s = 1$. The nontrivial zeros $\zeta(s)$ and the famous Riemann hypothesis can be explained from the functional equation too. Since $\Gamma(s)$ has a simple pole at $s = -n$, we see that $\zeta(-2n) = 0$ for each $n \geq 1$. We say that $-2, -4, -6, \ldots$ are the trivial zeros of $\zeta(s)$ and we call the other zeros of $\zeta(s)$ the nontrivial zeros. Since $\xi(s) = \xi(1-s)$, we have

$$\zeta(s) = \pi^{s-\frac{1}{2}} \frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)} \zeta(1-s).$$

This implies that if $s \neq -2n$, then $\zeta(s) = 0$ if and only if $\zeta(1-s) = 0$. In other words, the nontrivial zeros of $\zeta(s)$ are symmetric with respect to the vertical line $\sigma = \frac{1}{2}$. Since $\zeta(s) \neq 0$ for $\sigma \geq 1$, we know that $\zeta(s) \neq 0$ for $\sigma \leq 0$ and $s \neq -2n$ for any $n \geq 1$. So all the nontrivial zeros of $\zeta(s)$ lie in the strip $0 < \sigma < 1$. The Riemann hypothesis states that the nontrivial zeros all lie in the middle of the strip: the vertical line $\sigma = \frac{1}{2}$. That is, all nontrivial zeros of $\zeta(s)$ have real part $\sigma = \frac{1}{2}$. The strip $0 < \sigma < 1$ is called the *critical strip*, the line $\sigma = \frac{1}{2}$ is called the *critical line*, and the parts of $\mathbb{C}$ where there are no zeros of $\zeta(s)$ is called the *zero-free regions*.

Theorem 8.35 is good enough for the proof of the prime number theorem but to obtain a stronger form, we need to have a larger zero-free region such as $\sigma \geq 1 - g(t)$ where $g(t)$ is some function of $t$. We would like $g(t)$ to be arbitrarily close to $\frac{1}{2}$ as $g(t)$ determines the size of the error term in the estimate for $\pi(x)$. Below we state without proof, the classical zero-free region for $\zeta(s)$.

**Theorem 8.36.** *There exists an absolute constant* $c > 0$ *such that* $\zeta(s) \neq 0$ *for* $s \in \mathbb{C}$ *such that* $\sigma \geq 1 - \frac{c}{\log(|t|+4)}$.

For the proof of this theorem, see for example in Montgomery and Vaughan [**273**, p. 172], Ingham [**209**], or Tenenbaum [**407**]. In fact, Theorem 8.36 was first proved by de la Vallée Poussin in 1899. Since then many mathematicians including Hardy, Littlewood, Landau, Titchmarsh, Ingham, Vinogradov, Chudakov, Hua, Tatuzawa, Korobov, Richert, etc., have worked on this problem which lead to some improvement on the zero-free region for $\zeta(s)$. For more details on this problem, we refer the reader to Montgomery and Vaughan[**273**, pp. 192–198]. We let $\tau = |t| + 4$ and quote some parts of [**273**, pp. 193–194] as follows.

[Chudakov (1936)]

$$\zeta(s) \neq 0 \quad \text{for } s \in \mathbb{C} \text{ with } \sigma > 1 - \frac{c}{(\log \tau)^a} \text{ for some } a > 10/11. \tag{8.11}$$

[Titchmarsh (1951) and Tatuzawa (1952)]

$$\zeta(s) \neq 0 \quad \text{for } s \in \mathbb{C} \text{ with } \sigma > 1 - \frac{c}{(\log \tau)^{\frac{3}{4}} (\log \log \tau)^{\frac{3}{4}}}. \tag{8.12}$$

[Richert (1967)]

$$\zeta(s) \neq 0 \quad \text{for } s \in \mathbb{C} \text{ with } \sigma > 1 - \frac{c}{(\log \tau)^{\frac{2}{3}} (\log \log \tau)^{\frac{1}{3}}}. \tag{8.13}$$

These zero-free regions show that we are still very far from proving the Riemann hypothesis that the zero-free region should be $\sigma > \frac{1}{2}$. There are other approaches too. For instance, Hardy [**172**] and Hardy and Littlewood [**175**] showed that there are infinitely many nontrivial zeros of $\zeta(s)$ on the critical line. Selberg [**359**, **360**] improved it by proving that the nontrivial zeros of $\zeta(s)$ on the critical line have a positive proportion. More precisely, let $N(T)$ be the number of zeros $\rho = \beta + i\gamma$ of $\zeta(s)$ in the rectangle $0 < \beta < 1$, $0 < \gamma < T$ and let $N_0(T)$ be the number of zeros of the form $1/2 + i\gamma$ with $0 < \gamma < T$. Selberg proved that $N_0(T) \gg T \log \log T$ in [**359**] and then $N_0(T) \gg T \log T$ in [**360**]. Since $N(T) \sim \frac{T}{2\pi} \log \frac{T}{2\pi}$, Selberg's result implies that a positive proportion of the zeros are on the critical line. Then about 32 years later, Levinson [**243**] showed that this proportion is at least 1/3. For more details about this, we refer the reader to Montgomery and Vaughan [**273**, pp. 452–462]. For the current development of this approach, see the work of Conrey [**90**], Bui, Conrey, and Young [**65**], and Feng [**120**]. In particular, Feng obtained that $\liminf_{T \to \infty} N_0(T)/N(T) \geq 0.4128$, that is, there are at least 41.28% nontrivial zeros of $\zeta(s)$ on the critical line.

However, we should remark that this approach might be useless in view of applications even if we can prove that there are at least 99.99% nontrivial zeros of $\zeta(s)$ on the critical line. This is because we do not know the location of the remaining 0.01% of nontrivial zeros, and so the known zero-free regions for $\zeta(s)$ do not get wider, and thus we cannot reduce the error terms in the estimates for $\pi(x)$, $\theta(x)$, $\psi(x)$, and other related functions.

For a comprehensive introduction to basic properties of the Riemann zeta function, we refer the reader to the books by Titchmarsh [**411**] and Ivić [**211**]. For more information on the Riemann hypothesis, see the articles by Conrey [**91**, **92**]. Although the author of this book does not do research on the Riemann zeta function and $L$-functions, he believes that the reader can find more information by following the work of Professors A. Selberg, H. L. Montgomery, D. R. Heath-Brown, R. C. Vaughan, K. Soundararajan, B. Conrey, K. Matsumoto, V. Blomer, A. Ivić, D. A. Goldston, J. Steuding, V. Chandee, X. Li, and T. Srichan, and their coauthors, to name but a few.

Chapter 9

# Prime Number Theorem and Some Extensions

## 9.1. Introduction

Let us begin by recalling some of the results we obtained in Chapters 1–8. Let $\pi(x)$ and $\pi(x, q, a)$ be, respectively, the number of primes $p \le x$ and the number of primes $p \le x$ such that $p \equiv a \pmod{q}$. Euclid showed that there are infinitely many primes (Theorem 1.12 in Chapter 1), or equivalently, $\pi(x)$ tends to $\infty$ as $x \to \infty$. Euler provided another proof of this fact by considering $\zeta(s)$ for real $s > 1$ and proving that $\sum_p p^{-s}$ diverges as $s \to 1^+$. The natural problem then becomes that of understanding how the primes are distributed. If $(a, q) = 1$, does $\pi(x, q, a)$ diverge to $\infty$ as $x \to \infty$? How large or small is $\pi(x)$ when $x$ is large? Is $\pi(x, q, a) \sim \pi(x)/\varphi(q)$ if $(a, q) = 1$?

In 1808, about 60 years after Euler's proof of the divergence of the series $\sum p^{-1}$, Legendre conjectured that $\pi(x) \sim x/\log x$. Based on some numerical data and heuristic arguments, Gauss also proposed $\pi(x) \sim \mathrm{li}(x)$. Here and throughout this chapter,

$$\mathrm{li}(x) = \int_2^x \frac{1}{\log t}\,dt.$$

Since $\mathrm{li}(x) \sim x/\log x$, both hypotheses are equivalent, but one can show (see Section 9.3) that $\mathrm{li}(x)$ is better than $x/\log x$ in approximating $\pi(x)$.

In 1837, Dirichlet gave a complete answer to a problem on the distribution of primes in arithmetic progressions by proving a result (Theorem 7.23 in Chapter 7) which implies that if $a$ and $q$ are fixed and are coprime positive integers, then $\pi(x, q, a) \to \infty$ as $x \to \infty$. This result of Dirichlet is considered the birth of analytic number theory. In 1850, Chebyshev was the first to give a significant step toward the proof of Gauss and Legendre's conjecture by showing that $\pi(x) \asymp x/\log x$ (see Chapter 6). A few years later, Riemann (see Chapter 8) studied the properties of $\zeta(s)$ for $s \in \mathbb{C}$, obtained a functional equation for $\zeta(s)$, and proved that $\zeta(s)$ has an analytic continuation on $\mathbb{C} \setminus \{1\}$ and has a simple pole at $s = 1$ with residue 1. He also presented a new beautiful idea on a possible way to prove that $\pi(x) \sim x/\log x$ by giving an exact formula for $\pi(x)$ in terms of $\mathrm{li}(x)$ and the zeros of $\zeta(s)$. In 1896, about 40 years later, Hadamard and de la Vallée Poussin independently proved the validity of the estimate $\pi(x) \sim x/\log x$ and the result is now known as the prime number theorem (abbreviated as PNT).

Although the statement $\pi(x) \sim x/\log x$ is about integers, the original proofs by Hadamard and de la Vallée Poussin were based on Riemann's idea and heavily applied the knowledge from complex function theory. Since then several different proofs have been found. Our presentation in this text which is inspired by that of Newman uses complex functions too but this seems to be the simplest version in the literature. We give more details about this in Section 9.2.

Perhaps the most famous elementary proof of the PNT is that of Selberg [**358**] who discovered it in 1948. The proof of an arithmetic statement which does not involve complex analysis is usually said to be elementary though it may or may not be easy. So Selberg's proof is elementary but is not easy. For his work on the elementary proof of the PNT, the zeros of the Riemann zeta function, and sieve methods, Selberg won the Fields Medal in 1950. We give an outline of Selberg's elementary proof in Section 9.3. We remark that Erdös [**115**] also gave an elementary proof of the PNT, but his proof was based on Selberg's fundamental formula in [**358**].

However, the disadvantage of our simple proof and Selberg's elementary proof is that they do not lead to a strong form of the PNT. In Section 9.4, we give an outline on how to obtain better estimates than $\pi(x) \sim x/\log x$ and refer the reader to Montgomery and Vaughan [**273**] for more details. There are some generalizations of the PNT too. In

Section 9.5, we give the asymptotic formulas for the number of positive integers that are less than or equal to $x$ and have exactly $k$ prime factors, which may be considered as an extension of the PNT. Exercises are in Section 9.6. Some results concerning primes in arithmetic progressions, especially the approximations for $\pi(x, q, a)$, are given in Section 9.7. Notes on other topics are given in Sections 9.8 and 9.9, respectively. For a survey and a historical perspective, see the articles by Bateman and Diamond [**37**], Goldfeld [**143**, **144**], and references therein.

## 9.2. Proof of the Prime Number Theorem

In this section, we summarize the celebrated Wiener-Ikehara Tauberian theorem that is applied in countless settings in analytic number theory including the proof of the prime number theorem. For the original theorems by Wiener and by Ikehara, see [**434**] and [**208**], respectively. For more details about the Wiener-Ikehara theorem and related results, we refer the reader to Montgomery and Vaughan [**273**, pp. 259–266 and pp. 276–281]. Our proof of this theorem is inspired by a paper of Newman [**286**] as modified by Korevaar [**229**] and Zagier [**440**]. Below we state both the original version of Newman and the modification by Korevaar and Zagier but we give the proof only for the latter and leave the former as an exercise to the reader.

**Theorem 9.1.** (Newman [**286**]) *Suppose*

$$|a_n| \le 1 \ \ \textit{and} \ \ F(s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

*Then $F$ is analytic on the half-plane $\sigma > 1$. If $F$ has an analytic continuation onto the half-plane $\sigma \ge 1$, then $\sum_{n=1}^{\infty} a_n n^{-s}$ converges throughout $\sigma \ge 1$.*

**Theorem 9.2.** (Korevaar [**229**] and Zagier [**440**]) *Suppose $a_n \ge 0$ and $A(x) = \sum_{n \le x} a_n$. If the integral*

$$\int_1^{\infty} \frac{A(x) - x}{x^2} dx$$

*converges, then $A(x) \sim x$ as $x \to \infty$.*

**Proof.** Suppose that $A(x)$ is not asymptotic to $x$. Then there is a constant $\lambda > 1$ (or $\lambda < 1$) such that $A(x) \ge \lambda x$ (or $A(x) \le \lambda x$) for infinitely many values of $x$ tending to infinity. We consider the case $\lambda > 1$ (the case $\lambda < 1$ is similar). Since $A(x)$ is an increasing function of $x$, we see that for any of those $x$ with $A(x) \geq \lambda x$ and for $x \leq t \leq \lambda x$, we have $A(t) \geq A(x) \geq \lambda x$ and

$$\int_x^{\lambda x} \frac{A(t)-t}{t^2} dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2} dt = \int_1^{\lambda} \frac{\lambda x - vx}{(vx)^2} x\, dv$$
$$= \int_1^{\lambda} \frac{\lambda - v}{v^2}\, dv,$$

which is a positive quantity depending only on $\lambda$. Thus for such $x$, we have

$$\left| \int_x^{\infty} \frac{A(t)-t}{t^2} dt - \int_{\lambda x}^{\infty} \frac{A(t)-t}{t^2} dt \right| \geq \int_1^{\lambda} \frac{\lambda - v}{v^2} dv.$$

But the above integrals are tails of a convergent integral, and so both converge to zero as $x \to \infty$. This is a contradiction. ☐

**Theorem 9.3.** (Korevaar [**229**] and Zagier [**440**]) *Let $f$ be bounded on* $[0, \infty)$ *and integrable on every closed bounded subinterval of* $[0, \infty)$. *Let*

$$g(s) = \int_0^{\infty} f(x) e^{-sx} dx \quad \textit{for } \operatorname{Re}(s) > 0.$$

*If $g(s)$ has an analytic continuation to* $\operatorname{Re}(s) \geq 0$, *then $\int_0^{\infty} f(x)dx$ exists and equals* $g(0)$.

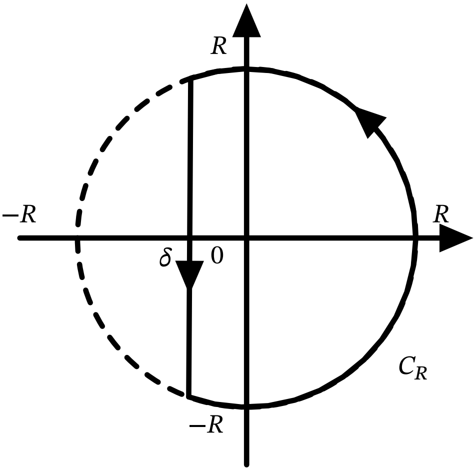
**Proof.** For $T > 0$, let

$$g_T(s) = \int_0^T f(x) e^{-sx} dx.$$

This converges for all values of $s \in \mathbb{C}$ and $g_T(s)$ is an entire function of $s$. We will show that

$$\lim_{T \to \infty} \int_0^T f(x) e^{-sx} dx = g(0).$$

Fix $R > 0$ and consider the positively oriented contour $C_R$ shown in the picture,



where $\delta > 0$ is chosen so that $g(s)$ is analytic on $C_R$. This can be done because the set $A = \{(0, y) \mid y \in [-R, R]\}$ is compact and for each point $a \in A$, there exists $\delta_a > 0$ such that $g(s)$ is analytic on $B(a, \delta_a) := \{s \in \mathbb{C} \mid |s - a| < \delta_a\}$. Then we have by Cauchy's integral formula

$$\frac{1}{2\pi i}\int_{C_R}(g(s) - g_T(s))e^{sT}\left(1 + \frac{s^2}{R^2}\right)\frac{1}{s}ds = g(0) - g_T(0). \tag{9.1}$$

As we traverse $C_R$ for $\mathrm{Re}(s) = \sigma > 0$, we observe that

$$|g(s) - g_T(s)| = \left|\int_T^\infty f(x)e^{-sx}dx\right| \ll \int_T^\infty e^{-\sigma x}dx = \frac{e^{-\sigma T}}{\sigma} \tag{9.2}$$

and we write $s = Re^{i\theta}$ to obtain

$$\left|\frac{e^{sT}}{s}\left(1 + \frac{s^2}{R^2}\right)\right| = e^{\sigma T}\left|\frac{1}{Re^{i\theta}} + \frac{e^{i\theta}}{R}\right| = \frac{2e^{\sigma T}|\cos\theta|}{R} \ll \frac{e^{\sigma T}|\sigma|}{R^2}. \tag{9.3}$$

Therefore the contribution to $g(0) - g_T(0)$ in (9.1) from this part of $C_R$ whose length is $\pi R$ is $O(1/R)$. Next we consider (9.1) on the path corresponding to $\mathrm{Re}(s) < 0$. First, by a similar calculation as in (9.2), we have

$$|g_T(s)| = \left|\int_0^T f(x)e^{-sx}dx\right| \ll \frac{e^{-\sigma T}}{-\sigma} \quad \text{for } \sigma = \mathrm{Re}(s) < 0.$$

Let $C_-$ be the path

$$C_R \cap \{s : \mathrm{Re}(s) < 0\}.$$

Since $g_T(s)$ is entire, we can deform the path $C_-$ to the part of the radial circular path corresponding to $s = Re^{i\theta}$ and $\pi/2 < \theta < 3\pi/2$ and we calculate as in (9.3) to obtain

$$\frac{1}{2\pi i}\int_{C_-} g_T(s)e^{sT}\left(1+\frac{s^2}{R^2}\right)\frac{1}{s}ds = O\left(\frac{1}{R}\right).$$

We are left with the problem of estimating

$$\frac{1}{2\pi i}\int_{C_-} g(s)e^{sT}\left(1+\frac{s^2}{R^2}\right)\frac{1}{s}ds. \tag{9.4}$$

Since $g(s)$ is analytic on $C_-$, we can find a constant $M_R$ depending only on $R$ such that

$$|g(s)| \le M_R$$

for all $s \in C_-$. In addition, for $s \in C_-$, $s = Re^{i\theta}$ or $s = -\delta + it$. When $s = Re^{i\theta}$, we can use the estimate as in (9.3). If $s = -\delta + it$, then

$$\left|\frac{e^{sT}}{s}\left(1+\frac{s^2}{R^2}\right)\right| \le e^{-\delta T}\left(\frac{1}{|s|}+\frac{|s|}{R^2}\right) \le e^{-\delta T}\left(\frac{1}{\delta}+\frac{1}{R}\right).$$

Therefore the integral in (9.4) is

$$\ll \frac{M_R}{R^2}\left|\int_{C_-} |\sigma| e^{\sigma T} ds\right| + \frac{RM_R e^{-\delta T}}{\delta} + M_R e^{-\delta T}.$$

Then

$$g(0) - g_T(0) \ll \frac{1}{R} + \frac{M_R}{R^2}\left|\int_{C_-} |\sigma| e^{\sigma T} ds\right| + \frac{RM_R e^{-\delta T}}{\delta} + M_R e^{-\delta T}. \tag{9.5}$$

On $C_-$, we have $\sigma < 0$ and $|\sigma|e^{\sigma T} \to 0$ uniformly on $C_-$ as $T \to \infty$. So as $T \to \infty$, the right-hand side of (9.5) converges to $\frac{1}{R}$. Then taking $R \to \infty$, we obtain $g(0) = \lim_{T\to\infty} g_T(0)$, as required. ☐

The Tauberian theorem can now be deduced from Theorem 9.3.

**Theorem 9.4.** *Let $a_n \ge 0$ and suppose that*

$$A(x) = \sum_{n \le x} a_n = O(x).$$

*Then the Dirichlet series $F(s) = \sum_{n=1}^{\infty} a_n/n^s$ converges absolutely for* $\mathrm{Re}(s) > 1$. *Assume that $F(s)$ has an analytic continuation to* $\mathrm{Re}(s) \ge 1$ *except for a simple pole at $s = 1$, with residue* 1. *Then $A(x) \sim x$ as $x \to \infty$.*

**Proof.** By partial summation,

$$\sum_{n\le x} a_n n^{-s} = \frac{A(x)}{x^s} + \frac{sx^{1-s}}{1-s} + \frac{s}{s-1} + s\int_1^x \frac{A(t)-t}{t^{s+1}}dt.$$

This implies that on the half-plane $\sigma > 1$, $\sum_{n=1}^{\infty} a_n n^{-s}$ converges absolutely, $F(s)$ is analytic, and

$$F(s) - \frac{s}{s-1} = s\int_1^\infty \frac{A(t)-t}{t^{s+1}}dt.$$

By changing $s$ to $s+1$ and $t = e^u$ in the integral, we have for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 0$,

$$F(s+1) - 1 - \frac{1}{s} = (s+1)\int_0^\infty \frac{A(e^u)-e^u}{e^u}e^{-us}du.$$

By the assumption $A(e^u) = O(e^u)$, we see that the function $f$ given by

$$f(u) = \frac{A(e^u)-e^u}{e^u}$$

is bounded on $[0,\infty)$ and integrable on every closed and bounded subinterval of $[0,\infty)$, and

$$\frac{F(s+1)-1-\frac{1}{s}}{s+1} = \int_0^\infty f(u)e^{-su}du. \tag{9.6}$$

The left-hand side of (9.6) is analytic for $\sigma > 0$. Since $F(s+1)$ has a simple pole at $s = 0$, we see that $F(s+1) - \frac{1}{s}$ is analytic at $s = 0$, and at any $s$ with $\sigma \ge 0$. So we can apply Theorem 9.3 to obtain that the integral

$$\int_0^\infty \frac{A(e^u)-e^u}{e^u}du = \int_1^\infty \frac{A(t)-t}{t^2}dt$$

converges. By Theorem 9.2, we deduce $A(x) \sim x$. ☐

Finally, after a lot of preparations throughout this and other chapters, we can now give a proof of the prime number theorem in its simplest form.

**Theorem 9.5.** (The Prime Number Theorem) *We have* $\psi(x) \sim x$, $\theta(x) \sim x$, *and* $\pi(x) \sim x/\log x$ *as* $x \to \infty$.

**Proof.** Since we already proved in Chapter 6 that the above three statements are equivalent, it is enough to show that $\psi(x) \sim x$. We recall from Corollary 8.30 that

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

which converges absolutely for all $s \in \mathbb{C}$ with $\sigma > 1$. We also recall from Theorem 8.35 that $\zeta(s) \neq 0$ for $s \in \mathbb{C}$ with $\sigma = 1$. Therefore by Theorems 8.32 and 8.35, we obtain that $\zeta'(s)$ is analytic on the half-plane $\sigma > 0$ except a pole of order 2, $\frac{1}{\zeta(s)}$ is analytic on the half-plane $\sigma \geq 1$, and their Laurent expansions are

$$\zeta'(s) = -\frac{1}{(s-1)^2} + a_0 + a_1(s-1) + \cdots, \quad \frac{1}{\zeta(s)} = (s-1) + b_2(s-1)^2 + \cdots.$$

Thus $-\frac{\zeta'(s)}{\zeta(s)}$ has an analytic continuation on $\sigma \geq 1$ except for a simple pole at $s = 1$. By Theorem 9.4, we obtain $\psi(x) \sim x$, as required. □

## 9.3. Elementary Proof of the Prime Number Theorem

In this section, we give an outline of Selberg's elementary proof of the prime number theorem [**358**]. We remind the reader again that elementary here does not mean easy; it only means there is no complex analysis involved in the proof.

As usual, let $\theta(x) = \sum_{p\leq x} \log p$. Selberg's idea is to prove that $\theta(x) \sim x$ by first establishing the following fundamental formula [**358**, Equations (2.8) and (2.9)]:

$$\sum_{p\leq x} (\log p)^2 + \sum_{pq\leq x} (\log p)(\log q) = 2x\log x + O(x) \tag{9.7}$$

$$\theta(x)\log x + \sum_{p\leq x} (\log p)\theta\left(\frac{x}{p}\right) = 2x\log x + O(x). \tag{9.8}$$

Here and throughout this section, $p$ and $q$ are primes. Other notations used in this book may be different from those used by Selberg. To prove (9.7), Selberg defined the functions $f$ and $g$ by

$$g(d,x) = g(d) = \mu(d)\left(\log\frac{x}{d}\right)^2$$

and

$$f(n,x) = f(n) = \sum_{d\mid n} g(d). \tag{9.9}$$

Selberg gave the exact formula for $f(n)$, which is also shown in Exercise 9.6.13, and calculated $\sum_{n\le x} f(n)$ in two ways which lead to

$$\sum_{n\le x} f(n) = x\sum_{d\le x}\frac{\mu(d)}{d}\left(\log\frac{x}{d}\right)^2 + O(x),$$
$$\sum_{n\le x} f(n) = \sum_{p\le x}(\log p)^2 + \sum_{pq\le x}(\log p)(\log q) + O(x), \quad \text{and thus}$$

(9.10)
$$\sum_{p\le x}(\log p)^2 + \sum_{pq\le x}(\log p)(\log q) = x\sum_{d\le x}\frac{\mu(d)}{d}\left(\log\frac{x}{d}\right)^2 + O(x).$$

The left-hand sides of (9.7) and (9.10) are the same, so it remains to evaluate the right-hand side of (9.10). To do this, he recalled the formulas for $\sum_{n\le y}\frac{1}{n}$ and $\sum_{n\le y}\frac{d(n)}{n}$, which imply

$$(\log y)^2 = 2\sum_{n\le y}\frac{d(n)}{n} + c_1\sum_{n\le y}\frac{1}{n} + c_2 + O\left(y^{-\frac{1}{4}}\right) \tag{9.11}$$

where $c_1$ and $c_2$ are absolute constants and $y \ge 1$. Then setting $y = \frac{x}{d}$ in (9.11), substituting it in (9.10), and recalling that $\mu * d = 1$ and $\sum_{d\le x}\mu(d)/d = O(1)$, Selberg obtained (9.7). Then by observing that

$$\sum_{p\le x}(\log p)^2 = \theta(x)\log x + O(x),$$

he obtained (9.8). We remark that the estimates for

$$\sum_{n\le y}\frac{1}{n} \quad\text{and}\quad \sum_{n\le y}\frac{d(n)}{n}$$

and the fact that $\mu * d = 1$ and $\sum_{d\le x}\mu(d)/d = O(1)$ are given in Theorem 4.14, Exercise 5.6.1, Theorem 2.17, and Exercise 5.6.8, respectively. Next, by (9.7) and partial summation, we get

$$\sum_{p\le x}\log p + \sum_{pq\le x}\frac{(\log p)(\log q)}{\log pq} = 2x + O\left(\frac{x}{\log x}\right).$$

This gives

$$\sum_{pq\le x}(\log p)(\log q)$$
$$= 2x\log x - \sum_{pq\le x}\frac{(\log p)(\log q)}{\log pq}\theta\left(\frac{x}{pq}\right) + O(x\log\log x).$$

Inserting this for the second term in (9.7), we get

$$\theta(x)\log x = \sum_{pq\le x} \frac{(\log p)(\log q)}{\log pq}\theta\left(\frac{x}{pq}\right) + O(x\log\log x). \tag{9.12}$$

Let $\theta(x) = x + R(x)$. Then (9.8) implies

$$R(x)\log x = -\sum_{p\le x}(\log p)R\left(\frac{x}{p}\right) + O(x).$$

From this point, Selberg established many other estimates for $R(x)$ such as

$$R(x)\log x = \sum_{pq\le x} \frac{(\log p)(\log q)}{\log pq}R\left(\frac{x}{pq}\right) + O(x\log\log x),$$

$$|R(x)| \le \frac{1}{\log x}\sum_{n\le x}\left|R\left(\frac{x}{n}\right)\right| + O\left(\frac{x\log\log x}{\log x}\right),$$

which eventually leads to the conclusion $R(x) = o(x)$. Hence

$$\theta(x) = x + R(x) = x + o(x),$$

which completes the proof.

After Hadamard and de la Vallée Poussin's articles were published, several different proofs were found, but before 1948, all of them used complex analysis. So it was natural to search for an elementary proof of the prime number theorem. Hardy and probably many other mathematicians thought that an elementary proof was unlikely to be discovered. However, such a proof was discovered by Selberg [**358**] in 1948. Erdös [**115**] also published an elementary proof of the PNT but his proof was also based on Selberg's fundamental formula which we show in (9.7) and (9.8). After Selberg and Erdös, there are many other elementary proofs too. In particular, Richter [**344**] has recently given a new elementary proof of the PNT using ergodic theory. We end this section by quoting Hardy's speech on the difficulty in finding an elementary proof of the PNT.

"No elementary proof of the prime number theorem is known, and one may ask whether it is reasonable to expect one. Now we know that the theorem is roughly equivalent to a theorem about an analytic function, the theorem that Riemann's zeta function has no roots on a certain line. A proof of such a theorem, not fundamentally dependent on the theory of functions, seems to me extraordinarily unlikely. It is rash to assert that a mathematical theorem cannot be proved in a particular way; but one thing seems quite clear. We have certain views about the logic of the theory; we think that some theorems, as we say "lie deep" and others nearer to the surface. If anyone produces an elementary proof of the prime number theorem, he will show that these views are wrong, that the subject does not hang together in the way we have supposed, and that it is time for the books to be cast aside and for the theory to be rewritten."

–G. H. Hardy (1921), Lecture to Mathematical Society of Copenhagen, Quoted in Goldfeld [**143**, **144**].

## 9.4. Stronger Forms of the Prime Number Theorem

It is often more convenient to use the prime number theorem in a stronger form such as $\theta(x) = x + O\left(xe^{-c\sqrt{\log x}}\right)$. In this section, we give an outline on how to obtain this version of the theorem and refer the reader to Montgomery and Vaughan [**273**, pp. 138–140 and pp. 179–182] for a complete proof. The first step is to recall Perron's formula as follows.

**Theorem 9.6.** (Perron's Formula) *Let* $\alpha(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ *be a Dirichlet series and let* $\sigma_c$ *be the abscissa of convergence of this series. Then for* $\sigma_0 > \max\{0, \sigma_c\}$ *and* $x > 0$*, we have*

$$\sum_{n\le x}{}' a_n = \lim_{T\to\infty} \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \alpha(s)\frac{x^s}{s} ds,$$

*where the notation* $'$ *on the sum means that if* $x$ *is an integer, then the last term in the sum is* $\frac{a_x}{2}$*.*

Let $\operatorname{si}(x) = -\int_x^{\infty} \frac{\sin u}{u} du$. Then $\operatorname{si}(x) \ll \min\{1, 1/x\}$ for $x > 0$ and $\operatorname{si}(x) + \operatorname{si}(-x) = -\pi$. A more useful version of Theorem 9.6 is as follows.

**Theorem 9.7.** *Suppose* $\alpha(s)$, $\sigma_c$, $\sigma_0$, *and* $x$ *are as in Theorem* 9.6. *Then*

$$\sum_{n\le x}{}' a_n = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \alpha(s)\frac{x^s}{s} ds + R,$$

*where R is equal to*

$$\frac{1}{\pi}\sum_{x/2<n<x} a_n \operatorname{si}\Bigl(T\log\frac{x}{n}\Bigr) - \frac{1}{\pi}\sum_{x<n<2x} a_n \operatorname{si}\Bigl(T\log\frac{x}{n}\Bigr) + O\left(\frac{4^{\sigma_0}+x^{\sigma_0}}{T}\sum_{n=1}^{\infty}\frac{|a_n|}{n^{\sigma_0}}\right).$$

*Moreover, we have*

$$R \ll \sum_{\substack{x/2<n<2x\\ n\neq x}} |a_n| \min\left\{1, \frac{x}{T|x-n|}\right\} + \frac{4^{\sigma_0}+x^{\sigma_0}}{T}\sum_{n=1}^{\infty}\frac{|a_n|}{n^{\sigma_0}}.$$

For the proof of Theorems 9.6 and 9.7, see [**273**, pp. 138–140]. By using Theorem 9.7 and the classical zero-free region (Theorem 8.36), one can obtain the prime number theorem in the following form (see [**273**, pp. 179–181]).

**Theorem 9.8.** *There is a constant* $c > 0$ *such that uniformly for* $x \geq 2$

$$\begin{aligned}\psi(x) &= x + O\left(xe^{-c\sqrt{\log x}}\right),\\ \theta(x) &= x + O\left(xe^{-c\sqrt{\log x}}\right),\\ \pi(x) &= \operatorname{li}(x) + O\left(xe^{-c\sqrt{\log x}}\right).\end{aligned}$$

We observe that for all $x \geq 3$, the error term $xe^{-c\sqrt{\log x}}$ is smaller than $x/(\log x)^A$ for any $A > 0$. So, for example, we can write

$$\theta(x) = x + O\left(x(\log x)^{-100}\right).$$

By integrating by parts $m$ times, we obtain an approximation for $\operatorname{li}(x)$ as given in Exercise 9.6.7. Combining it with Theorem 9.8, we obtain the formulas corresponding to $n = 2, 3$ as follows:

$$\begin{aligned}\pi(x) &= \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right) \quad \text{and}\\ \pi(x) &= \frac{x}{\log x} + \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3}\right).\end{aligned}$$

From this, one can easily see, as mentioned earlier in Section 9.1 that $\operatorname{li}(x)$ is better than $x/\log x$ in estimating $\pi(x)$.

The method used in the proof of Theorem 9.8 can be applied to many other situations too. As shown in [**273**, p. 182], we also have

$$\sum_{n\le x}\mu(n)\ll xe^{-c\sqrt{\log x}}\quad\text{and}\quad\sum_{n\le x}\frac{\mu(n)}{n}\ll e^{-c\sqrt{\log x}}.$$

Ingham ([**209**, pp. 60–65]; see also Titchmarsh [**411**, pp. 56–60]) developed a general result by which any given zero-free region of $\zeta(s)$ can be used to derive the associated bound for the error term in the prime number theorem. In particular, it can be shown that if (8.11) holds, then

$$\psi(x)=x+O\left(xe^{-c(\log x)^b}\right)$$

where $b=1/(1+a)$. Similarly, it follows from (8.13) that

$$\pi(x)=\mathrm{li}(x)+O\left(x\exp\left(-c(\log x)^{\frac{3}{5}}(\log\log x)^{-\frac{1}{5}}\right)\right).$$

For more details, see [**273**, pp. 194–198] and references therein. Finally, we state the strongest form of the PNT below (see [**273**, p. 419].

**Theorem 9.9.** *By assuming the Riemann hypothesis, we have for $x\ge 2$,*

$$\begin{aligned}\psi(x)&=x+O\left(\sqrt{x}(\log x)^2\right),\\ \theta(x)&=x+O\left(\sqrt{x}(\log x)^2\right),\\ \pi(x)&=\mathrm{li}(x)+O\left(\sqrt{x}\log x\right).\end{aligned}$$

Again, we remark that the Riemann hypothesis has not been proved yet. So the above result is still conditional.

## 9.5. Integers Having $k$ Prime Factors

We recall from Chapter 2 that $\Omega(n)$ and $\omega(n)$ are the number of prime divisors of $n$ counted with and without multiplicity, respectively. In this section, we are concerned with estimates for the functions $\pi_k$, $\pi_k^{\Omega}$, and $\pi_k^{\omega}$ defined by

$$\pi_k(x) = \sum_{\substack{n\le x\\ \omega(n)=\Omega(n)=k}} 1, \tag{9.13}$$

$$\pi_k^{\Omega}(x) = \sum_{\substack{n\le x\\ \Omega(n)=k}} 1, \tag{9.14}$$

$$\pi_k^{\omega}(x) = \sum_{\substack{n\le x\\ \omega(n)=k}} 1. \tag{9.15}$$

In general, $k$ may depend on $x$ but we mainly consider the case where $k$ is a fixed positive integer. Since $\omega(n) = \Omega(n)$ if and only if $n$ is squarefree, we see that $\pi_k$ counts the number of squarefree positive integers having exactly $k$ prime factors. The integers that are counted in (9.15) are of the forms $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where $a_1, a_2, \dots, a_k$ are positive integers and $p_1, p_2, \dots, p_k$ are distinct primes while those counted in (9.14) are of the similar form but $a_1, a_2, \dots, a_k$ are nonnegative and $a_1 + a_2 + \cdots + a_k = k$. When $k = 1$, $\pi_k^{\omega}(x)$ is the number of prime powers that are less than or equal to $x$ while $\pi_k^{\Omega}(x) = \pi_k(x) = \pi(x)$ is the number of primes that are less than or equal to $x$. So the estimates for these functions may be considered as extensions of the prime number theorem.

Let $\mathbb{P}$ be the set of prime numbers and let $\mathbb{P}^k$ be the set of ordered $k$-tuples of prime numbers. In order to obtain estimates for $\pi_k$, $\pi_k^{\Omega}$, and $\pi_k^{\omega}$, we first study the following functions defined by

$$a_k(n) = \sum_{\substack{(p_1,p_2,\dots,p_k)\in\mathbb{P}^k\\ p_1p_2\cdots p_k=n}} 1 \tag{9.16}$$

$$A_k(x) = \sum_{n\le x} a_k(n) = \sum_{\substack{(p_1,p_2,\dots,p_k)\in\mathbb{P}^k\\ p_1p_2\cdots p_k\le x}} 1 \tag{9.17}$$

$$L_k(x) = \sum_{\substack{(p_1,p_2,\dots,p_k)\in\mathbb{P}^k\\ p_1p_2\cdots p_k\le x}} \frac{1}{p_1 p_2 \cdots p_k} \tag{9.18}$$

$$\theta_k(x) = \sum_{\substack{(p_1,p_2,\dots,p_k)\in\mathbb{P}^k\\ p_1p_2\cdots p_k\le x}} \log(p_1 p_2 \cdots p_k). \tag{9.19}$$

The primes $p_1, p_2, \dots, p_k$ in the sums (9.16) to (9.19) may or may not be distinct and the rearrangement of them is counted as distinct. For example, if $n = 12$, then $n = (2)(2)(3) = (2)(3)(2) = (3)(2)(2)$, and therefore

$a_3(12) = 3$. By the uniqueness of prime factorization, we also see that $a_k(12) = 0$ for $k \neq 3$. This observation is recorded in the following lemma.

**Lemma 9.10.** *Let $n$ and $k$ be positive integers. Then the following statements hold.*

(i) *If $\Omega(n) = k$, then $a_k(n) > 0$ and $a_\ell(n) = 0$ for all $\ell \neq k$. Conversely, if $a_k(n) > 0$, then $\Omega(n) = k$ and $a_\ell(n) = 0$ for all $\ell \neq k$.*

(ii) *$\omega(n) = \Omega(n) = k$ if and only if $a_k(n) = k!$.*

(iii) *If $n = p_1^{a_1} p_2^{a_2} \cdots p_\ell^{a_\ell}$, $\Omega(n) = k$, and $p_1, p_2, \ldots, p_\ell$ are distinct primes, then*

$$a_k(n) = \frac{k!}{a_1!\, a_2! \cdots a_\ell!}.$$

**Proof.** The statement (i) follows from the fundamental theorem of arithmetic. For (ii), if $\omega(n) = \Omega(n) = k$, then $n$ is a squarefree number having exactly $k$ distinct prime factors $p_1, p_2, \ldots, p_k$ and therefore

$$a_k(n) = \text{ the number of permutations of } k \text{ objects } = k!\,.$$

Conversely, assume that $a_k(n) = k!$. Then $a_k(n) > 0$ so $\Omega(n) = k$. If $n$ is not squarefree, then there exists a prime $p$ such that $p^2 \mid n$ and so $a_k(n) \leq \frac{k!}{2!} < k!$, which is not the case. So $n$ is squarefree and thus $\omega(n) = \Omega(n) = k$. The statement (iii) follows from a counting formula: the number of permutations of $k$ objects, in which $a_1$ are of type 1, $a_2$ are of type 2, …, $a_\ell$ are of type $\ell$, where $a_1 + a_2 + \cdots + a_\ell = k$, is equal to

$$\frac{k!}{a_1!\, a_2! \cdots a_\ell!}. \qquad \square$$

**Lemma 9.11.** *Let $k$ be a fixed positive integer. Then*

$$k!\, \pi_k(x) \leq A_k(x) \leq k!\, \pi_k^\Omega(x).$$

*If $k \geq 2$, then*

$$0 \leq \pi_k^\Omega(x) - \pi_k(x) \leq \binom{k}{2} A_{k-1}(x).$$

**Proof.** By Lemma 9.10, we see that $a_k(n) \leq k!$ and if $\Omega(n) \neq k$, then $a_k(n) = 0$. In addition, if $\omega(n) = \Omega(n) = k$, then $a_k(n) = k!$. So we obtain

$$A_k(x) = \sum_{\substack{n\le x\\ \Omega(n)=k}} a_k(n) \ge \sum_{\substack{n\le x\\ \omega(n)=\Omega(n)=k}} a_k(n) = k!\,\pi_k(x), \quad \text{and}$$
$$A_k(x) = \sum_{\substack{n\le x\\ \Omega(n)=k}} a_k(n) \le \sum_{\substack{n\le x\\ \Omega(n)=k}} k! = k!\,\pi_k^{\Omega}(x).$$

Next assume that $k \ge 2$. Then by the definitions of $\pi_k^{\Omega}(x)$ and $\pi_k(x)$, we see that

$$0 \le \pi_k^{\Omega}(x) - \pi_k(x) = \sum_{\substack{n\le x\\ \Omega(n)=k\\ n \text{ is not squarefree}}} 1.$$

The integer $n$ that is not squarefree and $\Omega(n) = k$ is of the form $n = q_1q_2\cdots q_k = p_1p_2\cdots p_{k-2}p_{k-1}^2$, where $p_1,\dots,p_{k-1},q_1,\dots,q_k$ are primes not necessarily distinct. Therefore

$$\pi_k^{\Omega}(x) - \pi_k(x) \le \binom{k}{2} \sum_{\substack{(p_1,p_2,\dots,p_{k-1})\in\mathbb{P}^{k-1}\\ p_1p_2\cdots p_{k-1}\le x}} 1 = \binom{k}{2} A_{k-1}(x).$$

This completes the proof. □

**Lemma 9.12.** *Let k be a fixed positive integer. Then*

$$L_k(x) = (\log\log x)^k + O\left((\log\log x)^{k-1}\right).$$

*Define* $L_0(x) = 1$ *for all* $x \in (0,\infty)$. *Then*

$$L_k(x) = \sum_{p\le x} \frac{1}{p} L_{k-1}\left(\frac{x}{p}\right).$$

**Proof.** By the definition of $L_1(x)$ and by Mertens' theorem, we obtain $L_1(x) = \sum_{p\le x} \frac{1}{p} = \log\log x + O(1)$, and so

$$L_1\left(x^{\frac{1}{k}}\right) = \log\log x^{\frac{1}{k}} + O(1) = \log\log x + O(1).$$

In addition,

$$\begin{aligned}\left(L_1\left(x^{\frac{1}{k}}\right)\right)^k &= \left(\sum_{p\le x^{\frac{1}{k}}} \frac{1}{p}\right)^k \\ &= \sum_{p_1,p_2,\ldots,p_k\le x^{\frac{1}{k}}} \frac{1}{p_1p_2\cdots p_k} \le \sum_{p_1p_2\cdots p_k\le x} \frac{1}{p_1p_2\cdots p_k} \\ &= L_k(x) \le \sum_{p_1,p_2,\ldots,p_k\le x} \frac{1}{p_1p_2\cdots p_k} = \left(\sum_{p\le x}\frac{1}{p}\right)^k = \left(L_1(x)\right)^k.\end{aligned}$$

We have $(\log\log x + O(1))^k = (\log\log x)^k + O\left((\log\log x)^{k-1}\right)$. So the above inequality implies that $L_k(x) = (\log\log x)^k + O\left((\log\log x)^{k-1}\right)$. The other part is obvious when $k = 1$ and if $k \ge 2$, then

$$L_k(x) = \sum_{p\le x}\frac{1}{p}\sum_{p_1p_2\cdots p_{k-1}\le \frac{x}{p}} \frac{1}{p_1p_2\cdots p_{k-1}} = \sum_{p\le x}\frac{1}{p}L_{k-1}\left(\frac{x}{p}\right). \qquad \square$$

**Theorem 9.13.** *Let $k \ge 1$ be an integer. We have*

(i) $\theta_k(x) \sim kx(\log\log x)^{k-1}$,

(ii) $A_k(x) \sim \dfrac{kx(\log\log x)^{k-1}}{\log x}$,

(iii) $\pi_k^{\Omega}(x) \sim \dfrac{x(\log\log x)^{k-1}}{(k-1)!\log x}$,

(iv) $\pi_k(x) \sim \dfrac{x(\log\log x)^{k-1}}{(k-1)!\log x}$.

**Proof.** We first prove (i) by induction on $k$. The case $k = 1$ follows from the prime number theorem. So let $k \ge 1$ and assume that (i) holds for $k$. Then by Lemma 9.12, we obtain that

$$\begin{aligned}&\theta_{k+1}(x) - (k+1)x(\log\log x)^k \\ &\qquad = \theta_{k+1}(x) - (k+1)xL_k(x) + o\left(x(\log\log x)^k\right).\end{aligned}$$

So it suffices to show that

$$\theta_{k+1}(x) - (k+1)xL_k(x) = o(x(\log\log x)^k).$$

For convenience, let $A = \prod_{i=1}^{k+1} p_i$ and for each $j = 1, 2, \ldots, k+1$, let $A_j = \frac{A}{p_j}$. Then we obtain that $k\theta_{k+1}(x)$ is equal to

$$\begin{aligned}
&\sum_{\substack{(p_1,p_2,\ldots,p_{k+1})\in\mathbb{P}^{k+1}\\ p_1p_2\cdots p_{k+1}\le x}} \log(p_1p_2\cdots p_{k+1})^k \\
&= \sum_{\substack{(p_1,p_2,\ldots,p_{k+1})\in\mathbb{P}^{k+1}\\ p_1p_2\cdots p_{k+1}\le x}} \log\left(\frac{A}{p_1}\cdot\frac{A}{p_2}\cdots\frac{A}{p_{k+1}}\right) \\
&= \sum_{\substack{(p_1,p_2,\ldots,p_{k+1})\in\mathbb{P}^{k+1}\\ p_1p_2\cdots p_{k+1}\le x}} \sum_{j=1}^{k+1} \log\left(\frac{A}{p_j}\right) = \sum_{j=1}^{k+1}\sum_{p_j\le x}\sum_{A_j\le\frac{x}{p_j}} \log(A_j) \\
&= (k+1)\sum_{p\le x}\theta_k\left(\frac{x}{p}\right). \qquad (9.20)
\end{aligned}$$

By (9.20) and Lemma 9.12, we see that

$$\begin{aligned}
(9.21)\quad & k(\theta_{k+1}(x) - (k+1)xL_k(x)) \\
&= (k+1)\sum_{p\le x}\left(\theta_k\left(\frac{x}{p}\right) - \frac{kx}{p}L_{k-1}\left(\frac{x}{p}\right)\right).
\end{aligned}$$

By the induction hypothesis, we have

$$\theta_k(y) - kyL_{k-1}(y) = o\left(y(\log\log y)^{k-1}\right) \quad \text{as } y\to\infty.$$

Let $\varepsilon > 0$. Then there exists $y_0 > 2$ such that for all $y \ge y_0$, we have

$$|\theta_k(y) - kyL_{k-1}(y)| \le \varepsilon y(\log\log y)^{k-1}.$$

In addition, there exists a constant $c > 0$ such that

$$|\theta_k(y) - kyL_{k-1}(y)| \le c \text{ for all } y\in[0,y_0].$$

So we split the sum on the right-hand side of (9.21) into two parts: $p \le \frac{x}{y_0}$ and $\frac{x}{y_0} < p \le x$. In the second part, $\frac{x}{p} < y_0$ and therefore

$$\sum_{\frac{x}{y_0}<p\le x}\left(\theta_k\left(\frac{x}{p}\right) - \frac{kx}{p}L_{k-1}\left(\frac{x}{p}\right)\right) \le cx.$$

In the first part, as $x \to \infty$, we have

$$\begin{aligned}\sum_{p \le \frac{x}{y_0}} \left(\theta_k\left(\frac{x}{p}\right) - \frac{kx}{p} L_{k-1}\left(\frac{x}{p}\right)\right) &\le \sum_{p \le \frac{x}{y_0}} \varepsilon \frac{x}{p} \left(\log\log \frac{x}{p}\right)^{k-1} \\ &\le \varepsilon x (\log\log x)^{k-1} \sum_{p \le x} \frac{1}{p} \\ &\le 2\varepsilon x (\log\log x)^k.\end{aligned}$$

Therefore (9.21) implies that for all large $x$, we have

$$\begin{aligned}\theta_{k+1}(x) - (k+1)xL_k(x) &\le \left(1 + \frac{1}{k}\right)(cx + 2\varepsilon x(\log\log x)^k) \\ &\le 6\varepsilon x (\log\log x)^k.\end{aligned}$$

This shows that $\theta_{k+1}(x) - (k+1)xL_k(x) = o\left(x(\log\log x)^k\right)$ as required. For (ii), we write

$$\begin{aligned}\theta_k(x) = \sum_{n \le x} a_k(n) \log n &= \int_{1^-}^{x} \log t dA_k(t) \\ &= A_k(x) \log x - \int_1^x \frac{A_k(t)}{t} dt.\end{aligned}$$

By Lemma 9.11, the above integral is $O(x)$, which implies (ii). For (iii), we obtain from (ii) and Lemma 9.11 that

$$\pi_k^{\Omega}(x) \ge \frac{A_k(x)}{k!} \sim \frac{x(\log\log x)^{k-1}}{(k-1)! \log x},$$

and

$$\begin{aligned}\pi_k^{\Omega}(x) &\le \pi_k(x) + \binom{k}{2} A_{k-1}(x) \\ &\le \frac{A_k(x)}{k!} + \binom{k}{2} A_{k-1}(x) \sim \frac{x(\log\log x)^{k-1}}{(k-1)! \log x}.\end{aligned}$$

This implies (iii). Then (iii) and Lemma 9.11 imply (iv) and the proof is complete. □

Next we give the Hardy-Ramanujan inequality [**176**]. We follow the argument given by De Koninck and Luca [**102**].

**Theorem 9.14.** *There exist positive constants* $x_0$, $c_0$, *and* $c_1$ *such that uniformly for* $1 \le k \le 10 \log\log x$,

$$\pi_k^{\omega}(x) \le \frac{c_0 x(\log\log x + c_1)^{k-1}}{(k-1)! \log x} \quad \textit{for all } x > x_0.$$

**Proof.** Since the case $k = 1$ follows from Chebyshev's estimate, we assume that $k \ge 2$. Consider

$$\begin{aligned}\frac{(\log\log x + c_1)^{k-1}}{(k-1)!} &> \left(\frac{\log\log x}{k-1}\right)^{k-1} > \left(\frac{\log\log x}{10\log\log x}\right)^{k-1}\\ &> 10^{-10\log\log x} = \frac{1}{(\log x)^{10\log 10}}\end{aligned}$$

which holds for any $c_1 > 0$ and $2 \le k \le 10\log\log x$. Let $A = 10\log 10$. So if $\pi_k^{\omega}(x) < \frac{3x}{(\log x)^{A+1}}$, then we can take $c_0 = 3$ and we are done. So assume that $\pi_k^{\omega}(x) \ge \frac{3x}{(\log x)^{A+1}}$. Then

$$\begin{aligned}\pi_k^{\omega}(x)\log x &= \sum_{\substack{n\le x\\ \omega(n)=k}} \log\left(\frac{x}{n}\right) + \sum_{\substack{n\le x\\ \omega(n)=k}} \log n\\ &= \sum_{\substack{n\le x\\ \omega(n)=k}} \log\left(\frac{x}{n}\right) + \sum_{\substack{n\le x\\ \omega(n)=k}} \sum_{p^a\|n} \log(p^a)\\ &= s_1 + s_2, \qquad (9.22)\end{aligned}$$

say. Let $y = \frac{x}{(\log x)^{A+1}}$ and write $s_1 = s_1' + s_1''$ where

$$s_1' = \sum_{\substack{n\le y\\ \omega(n)=k}} \log\left(\frac{x}{n}\right) \text{ and } s_2'' = \sum_{\substack{y<n\le x\\ \omega(n)=k}} \log\left(\frac{x}{n}\right).$$

Then

$$s_1' \le \sum_{n\le y} \log x \le \frac{x}{(\log x)^A}.$$

If $y < n \le x$, then $\frac{x}{n} \le \frac{x}{y} \le (\log x)^{A+1}$ and so

$$s_1'' \le (A+1)(\log\log x)\pi_k^{\omega}(x).$$

Therefore

$$s_1 \le \frac{x}{(\log x)^A} + (A+1)(\log\log x)\pi_k^{\omega}(x). \qquad (9.23)$$

For $s_2$, we write $n = p^a m$, change the order of summation and use Chebychev's estimate to obtain

$$s_2 = \sum_{\substack{p^a m \le x \\ \omega(m)=k-1}} \log p^a = \sum_{\substack{m \le x \\ \omega(m)=k-1}} \sum_{p^a \le \frac{x}{m}} \log p^a \ll \sum_{\substack{m \le x \\ \omega(m)=k-1}} \frac{x}{m}. \tag{9.24}$$

By the multinomial theorem and Mertens' estimate, we obtain

$$\sum_{\substack{m \le x \\ \omega(m)=k-1}} \frac{1}{m} \le \frac{1}{(k-1)!} \left( \sum_{\substack{p,a \\ p^a \le x}} \frac{1}{p^a} \right)^{k-1} \ll \frac{1}{(k-1)!} (\log\log x + c_1)^{k-1}. \tag{9.25}$$

Let $c_0$ be the implied constant in (9.25). From (9.22), (9.23), (9.25), and (9.24), we obtain

$$\begin{aligned} &\pi_k^\omega(x) \log x \\ &\le \frac{x}{(\log x)^A} + (A+1)(\log\log x)\pi_k^\omega(x) + \frac{c_0 x (\log\log x + c_1)^{k-1}}{(k-1)!}. \end{aligned} \tag{9.26}$$

Since $\pi_k^\omega(x) \ge \frac{3x}{(\log x)^{A+1}}$, we see that for all large $x$,

$$\frac{x}{(\log x)^A} \le \frac{1}{3} \pi_k^\omega(x)(\log x) \quad \text{and} \quad (A+1)\log\log x \le \frac{1}{3}(\log x).$$

Therefore (9.26) implies that

$$\pi_k^\omega(x)(\log x) \le \frac{2}{3}\pi^\omega(x)(\log x) + \frac{c_0 x(\log\log x + c_1)^{k-1}}{(k-1)!}.$$

Hence

$$\pi_k^\omega(x) \le \frac{3c_0 x(\log\log x + c_1)^{k-1}}{(k-1)!\,(\log x)},$$

as required. ☐

It is possible to obtain an asymptotic formula for $\pi_k^\omega(x)$ but the proof is more complicated than that of the previous theorem and is beyond the scope of this book. We give such a formula below and refer the reader to the book by Tenenbaum [**407**, pp. 200–206] for the proof.

**Theorem 9.15.** *Let $A > 0$. There exist positive constants $c_1 = c_1(A)$ and $c_2 = c_2(A)$ such that, uniformly for $x \ge 3$, $1 \le k \le A \log\log x$, $N \ge 0$, we* *have*

$$\pi_k^{\omega}(x) = \frac{x}{\log x}\left(\sum_{j=0}^{N}\frac{P_{j,k}(\log\log x)}{(\log x)^j} + O_A\left(\frac{(\log\log x)^k}{k!}R_N(x)\right)\right)$$

*where* $P_{j,k}(X)$ *is a polynomial of degree at most* $k-1$ *and* $R_N(x) = e^{-c_1\sqrt{\log x}} + \left(\frac{c_2 N+1}{\log x}\right)^{N+1}$. *In particular, we have*

$$P_{0,k}(X) = \sum_{m+\ell=k-1}\frac{1}{m!\,\ell!}\lambda^{(m)}(0)X^{\ell},$$

*where* $\lambda(z) = \frac{1}{\Gamma(z+1)}\prod_p\left(1+\frac{z}{p-1}\right)\left(1-\frac{1}{p}\right)^z$. *Moreover, under the same conditions, we have*

$$\pi_k^{\omega}(x) = \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\left(\lambda\left(\frac{k-1}{\log\log x}\right) + O\left(\frac{k}{(\log\log x)^2}\right)\right).$$

**Theorem 9.16.** *Let* $\delta$ *satisfy* $0 < \delta < 1$. *There exist positive constants* $c_1 = c_1(\delta)$ *and* $c_2 = c_2(\delta)$ *such that, uniformly for* $x \ge 3$, $1 \le k \le (2-\delta)\log\log x$, $N \ge 0$, *we have*

$$\pi_k^{\Omega}(x) = \frac{x}{\log x}\left(\sum_{j=0}^{N}\frac{Q_{j,k}(\log\log x)}{(\log x)^j} + O_\delta\left(\frac{(\log\log x)^k}{k!}R_N(x)\right)\right)$$

*where* $Q_{j,k}$ *is a polynomial of degree at most* $k-1$ *and* $R_N(x) = e^{-c_1\sqrt{\log x}} + \left(\frac{c_2 N+1}{\log x}\right)^{N+1}$. *In particular, we have*

$$Q_{0,k}(X) = \sum_{m+\ell=k-1}\frac{1}{m!\,\ell!}\nu^{(m)}(0)X^{\ell},$$

*where* $\nu(z) = \frac{1}{\Gamma(z+1)}\prod_p\left(1-\frac{z}{p}\right)^{-1}\left(1-\frac{1}{p}\right)^z$. *Moreover, under the same conditions, we have*

$$\pi_k^{\Omega}(x) = \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\left(\nu\left(\frac{k-1}{\log\log x}\right) + O\left(\frac{k}{(\log\log x)^2}\right)\right).$$

As mentioned in the notes of Chapter 6, Rosser, Schoenfeld, Dusart, Axler, Ramaré, and many others have given explicit estimates for $\pi(x)$, $\theta(x)$, $\psi(x)$, and other closely related functions which are widely applicable. So it seems natural to consider explicit approximations for $\pi_k(x)$,

$\pi_k^{\Omega}(x)$, and $\pi_k^{\omega}(x)$ too. Landau [**238**] proved that for each $k \in \mathbb{N}$, we have

$$\pi_k(x) = \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\left(1 + O\left(\frac{1}{\log\log x}\right)\right),$$

and the same estimate also holds for $\pi_k^{\Omega}(x)$. Montgomery and Vaughan [**273**], Tenenbaum [**407**], and Hildebrand and Tenenbaum [**186**] provided more details on these and similar results. Bayless, Kinlaw, and Klyve [**38**] established explicit bounds for $\pi_k(x)$ and $\pi_k^{\Omega}(x)$ as follows: for $k \geq 2$ and $x \geq 3$,

$$\pi_k(x) \leq \frac{1.028x(\log\log x + 0.26153)^{k-1}}{(k-1)!\log x}.$$

For $x \geq 10^{12}$,

$$\begin{aligned} \pi_2^{\Omega}(x) \geq \pi_2(x) &\geq \frac{x(\log\log x + 0.1769)}{\log x}\left(1 + \frac{0.4232}{\log x}\right), \quad \text{and} \\ \pi_3^{\Omega}(x) &\leq \frac{1.028((\log\log x + 0.26153)^2 + 1.055852)}{2\log x}. \end{aligned}$$

Then Kinlaw [**225**] extended the above to

$$\begin{aligned} \pi_3^{\Omega}(x) &> \frac{x(\log\log x)^2}{2\log x} \quad \text{for } x \geq 500194, \text{ and} \\ \pi_3(x) &> \frac{x((\log\log x)^2 - 1)}{2\log x} \quad \text{for } x \geq 10203553. \end{aligned}$$

Currently, there are only a few results for $\pi_k(x)$, $\pi_k^{\Omega}(x)$, and $\pi_k^{\omega}(x)$ and research in this direction may be more active in the future. For more updates, we recommend the reader to follow the work of the aforementioned mathematicians.

Pollack [**300**] gave a generalization of the Hardy-Ramanujan inequality by replacing the summand 1 in $\pi_k^{\omega}(x)$ by any nonnegative multiplicative function. A function $L$ is said to be *log-like* if $L$ is increasing and positive on $[2, \infty)$ and there is a constant $k > 0$ such that for all $x \geq 2$ and $2 \leq w \leq \min(x/2, \sqrt{x})$,

$$\frac{L(x)}{L(x/w)} \leq 1 + \frac{k\log w}{\log x}. \tag{9.27}$$

For example, if $L(x) = (\log x)^A$ for any fixed $A > 0$, or

$$L(x) = (\log x)(\log\log 2x)(\log\log\log 8x) \quad \text{for all } x \geq 2,$$

then $L$ is log-like. One of Pollack's results is as follows.

**Theorem 9.17.** (Pollack [**300**, Theorem 2]) *Let $f$ be a nonnegative multiplicative function, and let $L$ be a log-like function, satisfying* (9.27) *for the constant $K$. For all $x \geq 2$ and all positive integers $k$,*

$$\sum_{\substack{n\leq x\\ \omega(n)=k}} f(n) \leq \frac{Ax}{L(x)} \sum_{j=0}^{k-1} \frac{\left(\frac{1}{2}BK\right)^{k-1-j}}{(k-1-j)!} \sum_{\substack{m\leq x\\ \omega(m)=j}} \frac{f(m)}{m},$$

*where*

$$A = \sup_{x^{1/2^k}\leq t\leq x} \frac{1}{t/L(t)} \sum_{p^v\leq t} f(p^v), \quad \textit{and}$$

$$B = \sup_{x^{1/2^k}\leq t\leq x} \frac{1}{\log t} \sum_{p^v\leq t} f(p^v)\frac{\log(p^v)}{p^v}.$$

For applications of this theorem, see also in the same paper [**300**].

## 9.6. Exercises

This is the last set of exercises in this book. Some problems follow from an application of the prime number theorem and some may be solved by using only an elementary argument. We mixed them together and hope that the reader will enjoy reading and solving them. Exercises 9.6.14 and 9.6.15 are taken from Apostol [**18**, pp. 101–102]. Exercise 9.6.16 is also adjusted from Apostol [**18**, p. 102]. Exercise 9.6.18 is from Vaughan's homework assignment and he refers it to Duncan, Rogers, and Orr (independently). See also Montgomery and Vaughan [**273**, p. 39]. For a lot more exercises, we recommend the problem books by Ram Murty [**332**], Ram Murty and Esmonde [**334**], Ram Murty, Dewar, and Graves [**333**], and Cojocaru and Ram Murty [**88**]. For a collection of unsolved problems in number theory, we refer the reader to the famous book of Guy [**164**].

9.6.1 Suppose that $\lim_{x\to\infty}\left(\sum_{p\leq x}\frac{\log p}{p} - \log x\right)$ exists. Use this and the result in Exercise 4.8.18 to show that $\theta(x) \sim x$. Similarly, if $\left(\sum_{n\leq x}\frac{\Lambda(n)}{n} - \log x\right)$ converges as $x \to \infty$, show that $\psi(x) \sim x$.

9.6.2 Let $A > 0$ be a constant. Use the PNT in a suitable form to show that

$$\sum_{p \le x} \frac{\log p}{p} = \log x + c_1 + O\left(\frac{1}{(\log x)^A}\right),$$

$$\sum_{n \le x} \frac{\Lambda(n)}{n} = \log x + c_2 + O\left(\frac{1}{(\log x)^A}\right),$$

where $c_1$ and $c_2$ are constants. Conclude that

$$\sum_{p \le x} (\log p)/p - \log x$$

and $\sum_{n \le x} \Lambda(n)/n - \log x$ converge as $x \to \infty$. This also gives a better approximation than those in Chapter 6.

9.6.3 Let $p_n$ be the $n$th prime. Prove that $p_n \sim n \log n$ as $n \to \infty$. Assuming the Riemann hypothesis, show that

$$p_n = n \log n + O(\sqrt{n}).$$

9.6.4 Show that

$$\sum_{n \le x} \mu(n) = o(x) \text{ and } \sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0.$$

9.6.5 Show that $\pi$, $\theta$, and $\psi$ are not rational functions. In other words, if $f = \pi$, $\theta$, or $\psi$, then there are no polynomials $A$ and $B$ such that $f(x) = A(x)/B(x)$ for all $x \in \mathbb{N}$.

9.6.6 This exercise shows an extension of some estimates given in Chapter 7. Let $a$ and $q$ be fixed coprime positive integers and let $A > 0$ be a constant. Show that for $x \ge 2$,

(i) $$\sum_{\substack{p \le x \\ p \equiv a \pmod q}} \frac{\log p}{p} = \frac{\log x}{\varphi(q)} + c_1 + O\left(\frac{1}{(\log x)^A}\right),$$

(ii) $$\sum_{\substack{n \le x \\ n \equiv a \pmod q}} \frac{\Lambda(n)}{n} = \frac{\log x}{\varphi(q)} + c_2 + O\left(\frac{1}{(\log x)^A}\right),$$

where $c_1$ and $c_2$ are constants which depend at most on $q$. (You can use the prime number theorem in any form except the one which depends on the Riemann hypothesis or any other unproved conjecture).

9.6.7 Prove the following statements.

(i) $\operatorname{li}(x) = \dfrac{x}{\log x} + \displaystyle\int_2^x \frac{dt}{(\log t)^2} - \frac{2}{\log 2}$ and for $n \geq 2$,

$$\operatorname{li}(x) = \frac{x}{\log x} \sum_{k=0}^{n-1} \frac{k!}{(\log x)^k} + n! \int_2^x \frac{dt}{(\log t)^{n+1}} + C_n,$$

where $C_n$ is a constant which does not depend on $x$.

(ii) For $x \geq 2$ and $n \in \mathbb{N}$,

$$\int_2^x \frac{dt}{(\log t)^n} = O\left(\frac{x}{(\log x)^n}\right).$$

(iii) For $x \geq 2$ and $n \in \mathbb{N}$,

$$\operatorname{li}(x) = \frac{x}{\log x} \sum_{k=0}^{n-1} \frac{k!}{(\log x)^k} + O\left(\frac{x}{(\log x)^{n+1}}\right),$$

where the implied constant depends on $n$ but not on $x$.

9.6.8 For each $n \in \mathbb{N}$ and $x \geq 2$, let

$$f_n(x) = \int_2^x \frac{t}{(\log t)^n} dt.$$

(i) Show that

$$f_n(x) = \frac{x^2}{2(\log x)^n} - \frac{2}{(\log 2)^n} + \frac{n}{2} \int_2^x \frac{t}{(\log t)^{n+1}} dt.$$

(ii) For each $x \in \mathbb{R}$ and $m \in \mathbb{N}$, define

$$(x)_0 = 1 \quad \text{and} \quad (x)_m = x(x+1)(x+2)\cdots(x+m-1).$$

Show that for each $k \in \mathbb{N}$, $f_n(x)$ is equal to

$$\frac{x^2}{2(\log x)^n} \sum_{m=0}^{k} \frac{(n)_m}{(2\log x)^m} - \frac{2}{(\log 2)^n} \sum_{m=0}^{k} \frac{(n)_m}{(2\log 2)^m} + \frac{(n)_{k+1}}{2^{k+1}} f_{n+k+1}(x).$$

(iii) Prove that $f_n(x) \ll x^2/(\log x)^n$.

(iv) Prove that

$$f_n(x) = \frac{x^2}{2(\log x)^n} - \frac{2}{(\log 2)^n} + O\left(\frac{x^2}{(\log x)^{n+1}}\right),$$

where the implied constant depends on $n$ but not on $x$.

9.6.9 Show that for $x \geq 2$,

$$\sum_{p \leq x} p = \frac{x^2}{2\log x} + O\left(\frac{x^2}{(\log x)^2}\right).$$

9.6.10 Let $a, q \in \mathbb{N}$ and $(a, q) = 1$ be fixed. Use Exercise 9.6.6 and the prime number theorem to show that

$$\pi(x, q, a) = \frac{\pi(x)}{\varphi(q)} + O\left(\frac{x}{(\log x)^2}\right).$$

Deduce that if $q$ is fixed and $x \to \infty$, then the primes $\leq x$ have equidistribution among each reduced residue classes modulo $q$.

9.6.11 Let $A > 0$ be a constant. Show that

$$\sum_{n \leq x} \Lambda(n)^3 = x(\log x)^2 - 2x\log x + 2x + O(x(\log x)^{-A}).$$

9.6.12 For $1 < y \leq x$, let $\Phi(x, y)$ be the number of positive integers $n \leq x$ such that every prime factor of $n$ is larger than $y$. That is

$$\Phi(x, y) = \sum_{\substack{n \leq x \\ p|n \to p > y}} 1.$$

(i) Using the inclusion-exclusion principle or otherwise, show that

$$\Phi(x, y) = x\prod_{p \leq y}\left(1 - \frac{1}{p}\right) + O\left(2^{\pi(y)}\right).$$

(ii) If $y = y(x) \leq \log x$ and $y(x) \to \infty$ as $x \to \infty$, show that as $x \to \infty$,

$$\Phi(x, y) = x\prod_{p \leq y}\left(1 - \frac{1}{p}\right) + O\left(x^{\frac{\log 2}{\log\log x}}\right).$$

9.6.13 Let $f$ be the function defined in (9.9). Show that

$$f(n, x) = \begin{cases} (\log x)^2, & \text{if } n = 1; \\ (\log p)(2\log x - \log p), & \text{if } n = p^a \text{ for some prime } p \\ & \text{and } a \geq 1; \\ 2(\log p)(\log q), & \text{if } n = p^a q^b \text{ for some primes } p, q \\ & \text{and } a, b \geq 1; \\ 0, & \text{otherwise.} \end{cases}$$

9.6.14 Let $n \geq 2$ and $a_1 < a_2 < \cdots < a_n \leq x$ be a set of positive integers such that no $a_i$ divides the product of the others. Prove that $n \leq \pi(x)$.

9.6.15 Let $s_n$ denote the sum of the first $n$ primes. Prove that for each $n \in \mathbb{N}$, the interval $(s_n, s_{n+1})$ contains a perfect square.

9.6.16 Given an integer $n > 1$ with two factorizations $n = \prod_{i=1}^{r} p_i$ and $n = \prod_{i=1}^{t} q_i$, where the $p_i$ are primes (not necessary distinct) and the $q_i$ are arbitrary integers $> 1$. Let $\alpha$ be a real number.

(i) If $\alpha \geq 1$ prove that

$$\sum_{i=1}^{r} p_i^{\alpha} \leq \sum_{i=1}^{t} q_i^{\alpha}.$$

(ii) Give an example to show that the inequality between $\sum_{i=1}^{r} p_i^{\alpha}$ and $\sum_{i=1}^{t} q_i^{\alpha}$ may be $<$ or $>$ if $\alpha \in (0, 1)$.

9.6.17 Suppose $n = 10^k a + m$ where $a, k, m \geq 1$ and $m < 10^k$. Prove the following statements.

(i) If $m$ is odd and $5 \nmid m$, then there are infinitely many primes $p$ such that $p \equiv m \pmod{10^k}$. Deduce that the last $k$ digits of $p$ and $n$ are the same.

(ii) If $m$ is even or $5 \mid m$, then there are infinitely many primes $p$ and $q$ such that $p + q \equiv m \pmod{10^k}$. Deduce that the last $k$ digits of $p + q$ are the same as those of $n$. Then give an example of an arithmetic progression whose terms are not a sum or a difference of two primes.

9.6.18 Let $Q(x)$ be the number of squarefree integers less than or equal to $x$. Prove the following statements.

(i) $Q(N) \geq N - \sum_{p} \left\lfloor \frac{N}{p^2} \right\rfloor$ for every positive integer $N$.

(ii) $$\sum_{p} \frac{1}{p^2} < \frac{1}{4} + \sum_{k=1}^{\infty} \frac{1}{(2k+1)^2}$$
$$< \frac{1}{4} + \frac{1}{2} \sum_{k=1}^{\infty} \left( \frac{1}{2k} - \frac{1}{2k+2} \right) = \frac{1}{2}.$$

(iii) $Q(N) > \frac{N}{2}$ for all positive integer $N$.

(iv) Every positive integer $n > 1$ can be written as a sum of two squarefree numbers.

## 9.7. Notes on Prime in Arithmetic Progressions

After proving the prime number theorem, we can ask a similar question on primes in arithmetic progressions. So the following functions are studied.

**Definition 9.18.** For each real number $x \geq 1$ and positive integers $a$ and $q$, let

$$\begin{aligned} \pi(x, q, a) &= \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1, \\ \theta(x, q, a) &= \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \log p, \\ \psi(x, q, a) &= \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n). \end{aligned}$$

By Dirichlet's theorem, we know that if $a$ and $q$ are fixed and $(a, q) = 1$, then $\pi(x, q, a)$, $\theta(x, q, a)$, and $\psi(x, q, a)$ diverge to $\infty$ as $x \to \infty$. By adapting the method used in the proof of the prime number theorem, one can prove the following result (see Exercises 9.6.6 and 9.6.10).

**Theorem 9.19.** *Let $a$ and $q$ be fixed and $(a, q) = 1$. Then as $x \to \infty$, we have*

$$\pi(x, q, a) \sim \frac{\pi(x)}{\varphi(q)}, \quad \theta(x, q, a) \sim \frac{x}{\varphi(q)}, \quad \textit{and } \psi(x, q, a) \sim \frac{x}{\varphi(q)}.$$

On one hand, Theorem 9.19 is satisfactory because the asymptotic formula does not depend on $a$, and so we see that the primes are equidistributed among each reduced residue classes modulo $q$. On the other hand, Theorem 9.19 is not satisfactory because $a$ and $q$ are required to be fixed. In some applications, it is often important to be able to vary $a$ and $q$ with $x$. The best unconditional result in this direction is given by Walfisz using a result of Siegel on $L(1, \chi)$.

**Theorem 9.20.** (Siegel-Walfisz Theorem) *There exists a constant* $c > 0$ *such that if* $A > 0$ *is a fixed real number, then*

$$\psi(x, q, a) = \frac{x}{\varphi(q)} + O_A\left(xe^{-c\sqrt{\log x}}\right),$$
$$\theta(x, q, a) = \frac{x}{\varphi(q)} + O_A\left(xe^{-c\sqrt{\log x}}\right),$$
$$\pi(x, q, a) = \frac{1}{\varphi(q)} \int_2^x \frac{1}{\log t} dt + O_A\left(xe^{-c\sqrt{\log x}}\right),$$

*uniformly in* $x \geq 2$, $q \leq (\log x)^A$, *and* $(a, q) = 1$. *The constant* $c$ *is computable but the implied constant in the error term, which depends only on* $A$, *is not computable.*

**Proof.** A proof of this theorem is given in the book by Montgomery and Vaughan [**273**, pp. 381–382]. Siegel's theorem on $L(1, \chi)$ can also be found in [**273**, pp. 372–374]. Without Siegel's theorem, this result holds uniformly but only for $q \leq (\log x)^{1-\delta}$ for some $\delta > 0$; see for example in [**98**, p. 123]. □

Although Theorem 9.20 allows us to vary $a$ and $q$ with $x$, the uniformity of $q$ is not large since it is limited to $q \leq (\log x)^A$. A much stronger (but conditional) result than Theorem 9.20 where the range of $q$ is $[2, x]$ is as follows.

**Theorem 9.21.** *Assume that the generalized Riemann hypothesis is true. Then*

$$\psi(x, q, a) = \frac{x}{\varphi(q)} + O\left(x^{\frac{1}{2}}(\log x)^2\right),$$
$$\theta(x, q, a) = \frac{x}{\varphi(q)} + O\left(x^{\frac{1}{2}}(\log x)^2\right),$$
$$\pi(x, q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + O\left(x^{\frac{1}{2}}(\log x)^2\right),$$

*uniformly in* $x \geq 2$, $2 \leq q \leq x$, *and* $(a, q) = 1$.

**Proof.** See in Montgomery and Vaughan [**273**, pp. 426–427]. □

Theorem 9.21 is strong but it is based on the unproved hypothesis. In some applications, it is enough to use the results which hold on average. The most important theorem in this direction was given by Bombieri [**57**] in 1965 and later improved by A. I. Vinogradov [**427**] in 1966. (This is not to be confused with the other well-known mathematician I. M. Vinogradov). Bombieri won the Fields Medal for this result in 1974.

**Theorem 9.22.** (Bombieri-Vinogradov Theorem) *If* $A > 0$ *is given, then there is a constant* $B = B(A) > 0$ *such that if* $Q \leq x^{\frac{1}{2}} (\log x)^{-B}$*, then*

$$\sum_{q \leq Q} \max_{y \leq x} \max_{(a,q)=1} \left| \psi(y, q, a) - \frac{y}{\varphi(q)} \right| \ll x(\log x)^{-A}. \tag{9.28}$$

Davenport [**98**], Gallagher [**140**], Montgomery [**272**] and Huxley [**206**] showed that we can take $B$ in Theorem 9.22 to be

$$B = 4A + 40, 16A + 103, A + 13, \text{ and } A + 10,$$

respectively. The best constants to date were obtained by Vaughan [**421**] where he showed that $B$ can be taken to be $A + \frac{7}{2}$. The quantity $|\psi(y, q, a) - y/\varphi(q)|$ in Theorem 9.22 can also be replaced by

$$\left| \theta(y, q, a) - \frac{y}{\varphi(q)} \right| \quad \text{and} \quad \left| \pi(y, q, a) - \frac{\pi(y)}{\varphi(q)} \right|.$$

One can say that, on average, the Bombieri-Vinogradov theorem is as good as the generalized Riemann hypothesis since if we substitute the formula

$$\psi(x, q, a) = \frac{x}{\varphi(q)} + O\left(\sqrt{x}(\log x)^2\right),$$

as shown in Theorem 9.21, in the sum of Theorem 9.22, we essentially obtain the same result up to a logarithmic factor. Nevertheless, the range of $q$ in Theorem 9.22 is restricted to $q \leq \sqrt{x}/(\log x)^B$, which is not good enough in some applications. One may expect that Bombieri-Vinogradov should be true for a larger range of $q$.

**Conjecture 9.23.** (Elliott-Halberstam Conjecture) Let $\varepsilon, A > 0$ be fixed. Then we have

$$\sum_{q \leq x^{1-\varepsilon}} \max_{y \leq x} \max_{(a,q)=1} \left| \psi(y, q, a) - \frac{y}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A},$$

$$\sum_{q \leq x^{1-\varepsilon}} \max_{y \leq x} \max_{(a,q)=1} \left| \theta(y, q, a) - \frac{y}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A},$$

$$\sum_{q \leq x^{1-\varepsilon}} \max_{y \leq x} \max_{(a,q)=1} \left| \pi(y, q, a) - \frac{\pi(y)}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

We are currently very far from proving the Elliott-Halberstam conjecture. The recent improvement on the Bombieri-Vinogradov theorem on the range of $q$ is given by Zhang [**442**] leading to his breakthrough on bounded gaps between primes:

$$\liminf_{n\to\infty}(p_{n+1}-p_n)\le 7\times 10^7.$$

We give more details about this in Section 9.9.

## 9.8. Analogues of the Bombieri-Vinogradov Theorem

In this section, we show some results analogous to the Bombieri-Vinogradov theorem, which have been obtained by various mathematicians. In particular, we quote and modify some sentences and formulas from Pongsriiam [**312**] and from Pongsriiam and Vaughan [**327–329**]. Consider the second moments of the error term in the estimate for $\psi(x,q,a)$. Let

$$V(x,Q)=\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\psi(x,q,a)-\frac{x}{\varphi(q)}\right|^2. \tag{9.29}$$

Results concerning $V(x,Q)$ first appeared in 1966 in the work of Barban [**36**], Davenport and Halberstam [**100**], and were later improved by Gallagher [**139**] in the following form: if $A>0$ is given and $Q\le x(\log x)^{-A}$, then

$$V(x,Q)\ll\frac{x^2}{(\log x)^{A-1}}. \tag{9.30}$$

The important point of this result is that the range of $q$ in (9.30) is wider than the one in the Bombieri-Vinogradov theorem. Then, in 1970, Montgomery [**271**] succeeded in replacing (9.30) by an asymptotic formula as follows: if $A>0$ and $Q\le x$, then

$$V(x,Q)=Qx\log Q+O\left(Qx+\frac{x^2}{(\log x)^A}\right).$$

Replacing $\psi(x,q,a)$ in (9.29) by $\theta(x,q,a)$, Hooley ([**193**] and [**194**]) introduced and developed in 1975 a simpler method which led him to a finer asymptotic formula than that of Montgomery. He obtained

$$V(x,Q)=Qx\log Q+cQx+O\left(Q^{\frac{5}{4}}x^{\frac{3}{4}}+\frac{x^2}{(\log x)^A}\right)\quad\text{for } Q\le x,$$

and by assuming the generalized Riemann hypothesis, the formula is

$$V(x,Q) = Qx\log Q + cQx + O\left(Q^{\frac{5}{4}}x^{\frac{3}{4}} + x^{\frac{3}{2}+\varepsilon}\right) \quad \text{for } Q \le x,$$

where $c$ is an absolute constant. Further developments occur in Friedlander and Goldston ([**135**] in 1996) and Goldston and Vaughan ([**146**] in 1997) and the methods have been broadened by Vaughan ([**423**, **424**] in 1998) and Hooley ([**195**, **197–201**] during 1975-2007) to study a wide range of sequences. The general principle is that the underlying arithmetic function, for example in the case of primes the von Mangoldt function, should satisfy an analogue of the Siegel–Walfisz theorem and there should be some understanding of the behavior of its $\ell_2$ mean. In particular, it should be constant on average, although not necessarily in $\ell_2$ mean, but the nature of the asymptotic formula obtained depends on the $\ell_2$ mean. The function $r(n)$, the number of representations of $n$ as a sum of two squares, does not fall within the orbit of the general results since while the average of $r(n)$ is a constant, that of $r(n)^2$ is large. Yet Dancs [**96**] showed that nevertheless there is an asymptotic formula for

$$\sum_{q\le Q}\sum_{a=1}^{q}\left|\sum_{\substack{n\le x\\ n\equiv a \pmod q}} r(n) - xf(q,a)\right|^2$$

where $f(q,a)$ is a suitable arithmetic function. Pongsriiam and Vaughan [**327–329**] investigated the corresponding expression in the case of $d(n)$, the number of positive divisors of $n$. They considered

$$A(x,q,a) = \sum_{\substack{n\le x\\ n\equiv a \pmod q}} d(n),$$

$$V(x,Q) = \sum_{q\le Q}\sum_{a=1}^{q} \left|A(x,q,a) - M(x,q,a)\right|^2, \tag{9.31}$$

where $M(x,q,a)$ is an appropriate approximating function given by

$$M(x,q,a) = \frac{x}{q}\sum_{r|q}\frac{c_r(a)}{r}\left(\log\frac{x}{r^2} + 2\gamma - 1\right).$$

As usual, $e(\alpha)$ denotes $e^{2\pi i\alpha}$ and $c_r(a)$ is Ramanujan's sum defined by $c_r(a) = \sum_b e(ba/r)$ where the sum is taken over positive integers $b \le r$ and $(b,r) = 1$. This has some general interest since it is an example in which the underlying function is not bounded on average. The function $A(x, q, a)$ has been widely studied; see for example in [**78**, **125**, **136**, **137**, **183**, **266**, **376**] and in [**219**, **247**, **327**] for some recent results. Blomer [**55**] and Banks, Heath-Brown, and Shparlinski [**31**] obtained the results concerning the innersum in (9.31). Motohashi [**277**] studied $V(x, Q)$ but only in the case $Q = x$. Pongsriiam and Vaughan [**327**, **328**] obtained a new and uniform estimate for $A(x, q, a)$ and used it to extend Motohashi's result to the general case $Q \leq x$ with a substantially smaller error term. For example, when $Q = x$, they obtained

$$V(x,x) = \frac{x^2}{\pi^2}(\log x)^3 + g_2x^2(\log x)^2 + g_1x^2\log x + g_0x^2 + O\left(x^{\frac{5}{3}+\varepsilon}\right),$$

where $g_0$, $g_1$, $g_2$, are absolute constants and can be computed explicitly. The formula for $V(x, Q)$ when $Q < x$ was also obtained but it is a bit too long to put in here. Based on Vaughan's method in [**423**, **424**] and the well-known circle method, Pongsriiam and Vaughan [**329**] also computed another second moment associated with $A(x, q, a)$ with a different approximating function. This method should allow us to calculate higher moments too and we hope to do it in the future. It should also be possible to obtain an error term smaller than $O\left(x^{5/3+\varepsilon}\right)$ but we do not have a proof yet. The corresponding investigation for other arithmetic functions such as the Euler function and the sum of divisors function may be even more challenging. We leave these problems to the interested reader.

## 9.9. Notes on Bounded Gaps Between Primes

There are several problems on primes which are still open. The Goldbach problem mentioned in the notes of Chapter 1 is to prove or disprove that every large even integer can be written as a sum of two primes. In this section, we give some information on another famous problem on primes: the twin prime conjecture. Let $p_n$ be the $n$th prime. If $p_{n+1} - p_n = 2$, then we say that $p_n$ and $p_{n+1}$ are twin primes. It is conjectured that there are infinitely many pairs of twin primes but this has been open for more than 150 years. According to Mackenzie [**255**], it is unclear, when and by whom, this conjecture was first proposed, but its goes back at least as far as 1849 when Polignac published a conjecture that for every positive even integer $k$, there are infinitely many $p$ such that $p$ and $p + k$ are both primes. Before 2013, there was no proof that there exists even one such $k$ for which Polignac's conjecture is true. The twin prime conjecture corresponding to the special case $k = 2$ is also considered extremely difficult. Then, in 2013, Zhang [**442**] made a breakthrough by proving that there is in fact one such $k$ and that $k \leq 7 \times 10^7$.

For convenience, for each $m \geq 1$, let

$$H_m = \liminf_{n\to\infty}(p_{n+m} - p_n).$$

The twin problem is to show that $H_1 = 2$ and what Zhang proved is that $H_1 \leq 7 \times 10^7$. Before Zhang, we only knew from the result of Goldston, Pintz, and Yildirim [**145**] that

$$\liminf_{n\to\infty}((p_{n+1} - p_n)/\log p_n) = 0,$$

but after Zhang, many mathematicians including Tao and the members of the Polymath8 project have worked on this problem. They [**304**] first obtained $H_1 \leq 4648$. See also an improved version of [**304**] in [**305**] and [**306**]. Shortly after that, Maynard [**267**] reduced it to $H_1 \leq 600$ and also to $H_1 \leq 12$ if the Elliott-Halberstam conjecture is true. It was also the first time that we knew anything on the finiteness of $H_m$ for $m \geq 2$ when Maynard [**267**] showed that there exists a computable positive constant $C$ such that $H_m \leq Cm^3e^{4m}$ for all $m \geq 1$. After that, the members of the Polymath8 project [**307**] improved it further to $H_1 \leq 246$ and $H_m \leq Cme^{am}$ where $a = 4 - 28/157$. By assuming the Elliott-Halberstam conjecture, they [**307**] also proved that $H_m \leq Cme^{2m}$. For more information, we refer the reader to [**267**, **304–307**], references therein, and also in the online blog of Tao. In addition, Vatwani [**420**] developed an axiomatic formulation of the higher rank version of the classical Selberg sieve, and used it to give a simplified proof of the Zhang and Maynard-Tao results on bounded gaps between primes. Moreover, Ram Murty and Vatwani [**335**] also extended Vatwani's result in [**420**] by adding an additive twist and applied this new version to improve the results of Heath-Brown and Ho-Tsang on almost prime $k$-tuples. The reader can find more information about this in [**335**, **420**] and references therein. Finally, we remark that Maynard won the Fields Medal in 2022 for his contributions to the prime number theory.

## Chapter 10

# Introduction to Other Topics

In this chapter, we give a basic idea in additive number theory and sieve methods. In particular, we talk about Brun's sieve, Selberg's sieve, Schnirelmann's basis theorem, twin primes conjecture, Waring's problem, and the circle method. Since there are already many excellent monographs on these topics and we intend to keep the material short and simple, we sometimes show only an outline of a proof and refer the readers to other textbooks for details. The Sieve Methods by Halberstam and Richert [**167**] and the Opera de Cribo by Friedlander and Iwaniec [**138**] are famous classic references for sieve theory. However, we also use the books by Cojocaru and Murty [**88**], Halberstam and Roth [**168**], Hua [**203**], Montgomery and Vaughan [**273**], and Pollack [**299**] as references in our presentation. For additive number theory and the circle method, we follow Davenport [**99**], Halberstam and Roth [**168**], Hua [**203**], Nathanson [**281, 283**], Vaughan [**422**], and Vaughan and Wooley [**426**]. We begin with sieves in the next section.

## 10.1. Idea of Sieves

Recall that a positive integer $n > 1$ is prime if and only if $p$ does not divide $n$ for every prime $p \le \sqrt{n}$. This leads to Eratosthenes' method for finding all primes not exceeding $x$. We first list all integers in $[2, x]$, and for each $p \le \sqrt{x}$, we cross out all multiples of $p$ except $p$. The numbers remaining in the list are exactly the primes in $[2, x]$. This sieving process is usually called the sieve of Eratosthenes.

Now let us try to count the number of primes $\leq x$ by using the idea of sieves. Let $z$ be a parameter to be determined later (in Eratosthenes' sieve, let $z = \sqrt{x}$) and let $\pi(x, z)$ be the number of $n \leq x$ that is not divisible by any prime $\leq z$, that is

$$\pi(x, z) = \sum_{\substack{n \leq x \\ p \mid n \to p > z}} 1.$$

Noting that 1 is counted in $\pi(x, z)$, we see that if $z = \sqrt{x}$, then $\pi(x, z) - 1$ is the number of primes in the interval $(\sqrt{x}, x]$ and

$$\pi(x) = \pi(\sqrt{x}) + \pi(x, z) - 1.$$

For any $z \geq 1$, if $p$ is a prime, then either $p \leq z$ or $p$ is not divisible by any prime not exceeding $z$, and so we have $\pi(x) \leq z + \pi(x, z)$. If $r = \pi(z)$ and $p_1 < p_2 < \cdots < p_r$ are the primes less than or equal to $z$, then by the inclusion-exclusion principle, we obtain

$$\begin{aligned}\pi(x, z) &= \lfloor x \rfloor - \sum_{1 \leq i \leq r} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{1 \leq i < j \leq r} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \cdots \\ &\quad + (-1)^r \left\lfloor \frac{x}{p_1 p_2 \cdots p_r} \right\rfloor \\ &= \lfloor x \rfloor - \sum_{p \leq z} \left\lfloor \frac{x}{p} \right\rfloor + \sum_{p_i < p_j \leq z} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \cdots + (-1)^r \left\lfloor \frac{x}{p_1 p_2 \cdots p_r} \right\rfloor.\end{aligned}$$

Let $P = P(z) = \prod_{p \leq z} p$. Then $\pi(x, z)$ can also be written as

$$\pi(x, z) = \sum_{d \mid P(z)} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = x \prod_{p \leq z} \left(1 - \frac{1}{p}\right) + O\left(2^{\pi(z)}\right).$$

Taking $z = \log x$ and using Mertens' theorem, we obtain

$$\pi(x, z) \sim \frac{e^{-\gamma} x}{\log \log x} \quad \text{and} \quad \pi(x) \ll \frac{x}{\log \log x}.$$

Since we already know that $\pi(x) \sim x / \log x$, the bound $\pi(x) \ll x / \log \log x$ given above may seem useless, but the method leading us to this bound is still interesting because it is not difficult and uses only Eratosthenes' sieve, the inclusion-exclusion principle, and Mertens' theorem. Besides, this idea can be extended to a general situation such as the counting of twin primes, the number of ordered representations of a positive integer as a sum of two primes, and many other counting problems. Let us now introduce the following standard notation, which is used throughout Sections 10.2 and 10.3.

Let $\mathcal{A}$ be a finite set of integers, $\mathcal{P}$ a finite set of primes, and $S(\mathcal{A}, \mathcal{P})$ the number of elements in $\mathcal{A}$ that are not divisible by any prime in $\mathcal{P}$. Equivalently,

$$S(\mathcal{A}, \mathcal{P}) = \#\{a \in \mathcal{A} \mid \ (a, p) = 1 \text{ for all primes } p \in \mathcal{P}\}.$$

We sometimes allow $\mathcal{P}$ to be an infinite set of primes, and define $P(z)$ to be the product of all primes in $\mathcal{P}$ that are less than or equal to $z$, and let $S(\mathcal{A}, \mathcal{P}, z)$ be the number of elements of $\mathcal{A}$ that are coprime to $P(z)$. That is,

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p \le z}} p \text{ and } S(\mathcal{A}, \mathcal{P}, z) = \#\{a \in \mathcal{A} \mid \gcd(a, P(z)) = 1\}.$$

In addition, let

$$A_d = \#\{a \in \mathcal{A} \mid a \text{ is divisible by } d\}.$$

The idea of sieves is to estimate $S(\mathcal{A}, \mathcal{P})$ for any $\mathcal{A}$ and $\mathcal{P}$ that are of interest. For example, if

$$\mathcal{A} = \{n \in \mathbb{N} \mid n \le x\} \text{ and } \mathcal{P} = \{p \mid p \text{ is a prime and } p \le z\},$$

then $S(\mathcal{A}, \mathcal{P}) = \pi(x, z)$; if $\pi_2(x)$ is the number of primes $p \le x$ such that $p + 2$ is also a prime, $\mathcal{A} = \{n(n+2) \mid n \le x\}$, and $\mathcal{P}$ is the same as above, then $\pi_2(x) \le z + S(\mathcal{A}, \mathcal{P})$, and so an appropriate upper bound for $S(\mathcal{A}, \mathcal{P})$ may give a good upper bound for the number of twin primes $\le x$. We give more details on an estimate for $\pi_2(x)$ in the next section.

## 10.2. Brun's Sieve

In this section, we give the proof of Brun's sieve and applications to twin primes problem. We begin with a lemma on binomial coefficients.

**Lemma 10.1.** *If $\ell \ge 1$ and $0 \le m \le \ell$, then*

$$\sum_{k=0}^{m} (-1)^k \binom{\ell}{k} = (-1)^m \binom{\ell - 1}{m}.$$

**Proof.** This follows by induction on $m$ and the well-known Pascal triangle identity. The details are left as an exercise to the reader. □

Next, we apply the inclusion-exclusion principle and Lemma 10.1 to obtain the following inequality which may be considered as a simple form of Brun's sieve.

**Theorem 10.2.** *Let $X$ be a nonempty finite set, and let $P_1, \dots, P_r$ be properties that elements of $X$ may have. For each subset $I$ of $\{1, 2, \dots, r\}$, let $N(I)$ denote the number of elements of $X$ that have each of the properties indexed by the elements of $I$, where $N(\phi)$ is defined to be $|X|$. Let $N_0$ be the number of elements of $X$ with none of these properties. Then we have*

$$N_0 = \sum_{k=0}^{r} (-1)^k \sum_{\substack{I \subseteq \{1,2,\dots,r\} \\ |I|=k}} N(I) = \sum_{I \subseteq \{1,2,\dots,r\}} (-1)^{|I|} N(I). \tag{10.1}$$

*Furthermore, if $m$ is a nonnegative even integer, then*

$$N_0 \le \sum_{k=0}^{m} (-1)^k \sum_{\substack{I \subseteq \{1,2,\dots,r\} \\ |I|=k}} N(I), \tag{10.2}$$

*if $m$ is a nonnegative odd integer, then*

$$N_0 \ge \sum_{k=0}^{m} (-1)^k \sum_{\substack{I \subseteq \{1,2,\dots,r\} \\ |I|=k}} N(I). \tag{10.3}$$

**Proof.** We can consider $X$ as the universal set and for each $i = 1, 2, \dots, r$, the set $A_i$ is the set of all elements in $X$ having property $P_i$. So $N_0 = |A_1^c \cap A_2^c \cap \cdots A_r^c|$ which can be obtained by the inclusion-exclusion principle. This gives (10.1). In addition, if we recall the basic idea of the inclusion-exclusion principle, we know that if $m = 0$, then the right-hand side of (10.2) really overcounts $N_0$; if $m = 1$, then the right-hand side of (10.3) underestimates $N_0$; and so on. This idea leads to (10.2) and (10.3). More precisely, suppose that $x \in X$ has exactly $\ell$ of the properties $P_1, \dots, P_r$. If $\ell = 0$, then $x$ is counted once by both $N_0$ and the sum in (10.2) and (10.3). If $\ell \ge 1$, then $x$ is not counted by $N_0$, and is counted by the sum in (10.2) and (10.3) with weight

$$\sum_{k=0}^{m} (-1)^k \binom{\ell}{k} \begin{cases} \ge 0, & \text{if } m \text{ is even;} \\ \le 0, & \text{otherwise,} \end{cases}$$

where the inequality for the above sum follows from Lemma 10.1. Summing over $x \in X$ gives the desired result. □

We recall that we let $\mathcal{A}$ be a finite set of integers, $\mathcal{P}$ a finite set of primes, and

$$S(\mathcal{A},\mathcal{P}) = \#\{a \in \mathcal{A} \mid \gcd(a,P) = 1\},$$

where $P = \prod_{p\in\mathcal{P}} p$. In addition, let

$$A_d = \#\{a \in \mathcal{A} \mid a \text{ is divisible by } d\}.$$

For instance, if $\mathcal{A}$ is the set of positive integers $n \le x$, then

$$A_d = \left\lfloor \frac{x}{d} \right\rfloor = \frac{x}{d} + O(1).$$

In a general case, we try to estimate $A_d$ in a similar way. So we assume the existence of a multiplicative function $\alpha$ taking values in $[0,1]$ such that

$$A_d = X\alpha(d) + r(d),$$

where $X$ is approximately equal to $|\mathcal{A}|$ and $r(d)$ is defined so that the above equality holds. When $\mathcal{A}$ is the set of positive integers $n \le x$, an obvious choice is to choose $X = x$, $\alpha(d) = \frac{1}{d}$, and $r(d) = -\left\{\frac{x}{d}\right\}$, so that $A_d = \left\lfloor \frac{x}{d} \right\rfloor = X\alpha(d) + r(d)$. Using the above notation, we can rewrite Theorem 10.2 in the following version of Brun's sieve.

**Theorem 10.3.** (Brun's Sieve) *If $m$ is a nonnegative even integer, then*

$$\sum_{d|P,\ \omega(d)\le m-1} \mu(d)A_d \le S(\mathcal{A},\mathcal{P}) \le \sum_{d|P,\ \omega(d)\le m} \mu(d)A_d.$$

**Proof.** Let $p_1,\dots,p_r$ be the primes in $\mathcal{P}$, and let $P_i$ be the property of being divisible by $p_i$. Then $S(\mathcal{A},\mathcal{P})$ is the number of elements of $\mathcal{A}$ possessing none of the $P_i$. Considering the set $X$ in Theorem 10.2 as $\mathcal{A}$, we see that $S(\mathcal{A},\mathcal{P})$ is the number $N_0$ in Theorem 10.2. We note that the result is obvious when $m = 0$, so we assume that $m \ge 2$. Then

$$\begin{aligned}\sum_{\substack{d|P\\ \omega(d)\le m}} \mu(d)A_d &= \sum_{k=0}^{m} \sum_{\substack{d|p_1p_2\cdots p_r\\ \omega(d)=k}} \mu(d)A_d = \sum_{k=0}^{m}(-1)^k \sum_{\substack{d|p_1p_2\cdots p_r\\ \omega(d)=k}} A_d\\ &= \sum_{k=0}^{m}(-1)^k \sum_{|I|=k} N(I),\end{aligned}$$

where $N(I)$ is the number of elements in $\mathcal{A}$ having properties indexed by $I \subseteq \{1, 2, \ldots, r\}$. Similarly,

$$\sum_{\substack{d|P \\ \omega(d)\le m-1}} \mu(d)A_d = \sum_{k=0}^{m-1} (-1)^k \sum_{|I|=k} N(I).$$

So the upper and lower bounds follow from (10.2) and (10.3). $\square$

Next, we give another version of Brun's sieve, which will be used to obtain an upper bound for $\pi_2(x)$, the number of twin primes not exceeding $x$. We use the same notation as before, but we state them again for clarity.

**Theorem 10.4.** (Brun's Sieve) *Let $\mathcal{A}$ be a finite set of integers, $\mathcal{P}$ a finite set of primes, $P = \prod_{p\in\mathcal{P}} p$, and $A_d$ the number of elements in $\mathcal{A}$ that are divisible by d. For each $d \mid P$, suppose $A_d = X\alpha(d) + r(d)$ for some $X$, $\alpha(d)$, and $r(d)$ such that $X \ge 0$, $\alpha(d) \in [0, 1]$, and $\alpha$ is a multiplicative function. Then for every even integer $m \ge 0$, we have*

$$S(\mathcal{A}, \mathcal{P}) = X \prod_{p\in\mathcal{P}} (1 - \alpha(p)) + O\left( \sum_{d|P,\ \omega(d)\le m} |r(d)| \right) + O\left( X \sum_{d|P,\ \omega(d)\ge m} \alpha(d) \right),$$

*where the implied constants are absolute.*

**Proof.** From Theorem 10.3, we have

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}) &= \sum_{\substack{d|P \\ \omega(d)\le m}} \mu(d)A_d + O\left( \sum_{\substack{d|P \\ \omega(d)=m}} A_d \right) \\ &= \sum_{\substack{d|P \\ \omega(d)\le m}} \mu(d)\left(X\alpha(d) + r(d)\right) + O\left( \sum_{\substack{d|P \\ \omega(d)=m}} A_d \right) \\ &= X \sum_{\substack{d|P \\ \omega(d)\le m}} \mu(d)\alpha(d) + O\left( \sum_{\substack{d|P \\ \omega(d)\le m}} |r(d)| \right) + O\left( \sum_{\substack{d|P \\ \omega(d)=m}} A_d \right). \end{aligned}$$

The second error term is

$$\ll \sum_{d|P,\, \omega(d)=m} X\alpha(d) + \sum_{d|P,\, \omega(d)=m} |r(d)|.$$

Therefore

$$\begin{aligned} &S(\mathcal{A}, \mathcal{P}) \\ &\qquad = X \sum_{\substack{d|P \\ \omega(d)\le m}} \mu(d)\alpha(d) + O\left( \sum_{\substack{d|P \\ \omega(d)\le m}} |r(d)| \right) + O\left( \sum_{\substack{d|P \\ \omega(d)=m}} X\alpha(d) \right). \end{aligned}$$

Writing the main term as

$$\begin{aligned} &X \sum_{d|P} \mu(d)\alpha(d) + O\left( \sum_{\substack{d|P \\ \omega(d)>m}} X\alpha(d) \right) \\ &\qquad\qquad = X \prod_{p\in\mathcal{P}} (1-\alpha(p)) + O\left( \sum_{\substack{d|P \\ \omega(d)>m}} X\alpha(d) \right), \end{aligned}$$

we obtain the desired result. □

With the version of Brun's sieve given in Theorem 10.4, we now give an upper bound for $\pi_2(x)$, the number of primes $p \le x$ such that $p+2$ is also prime. We remark that a better bound $\pi_2(x) \ll x/(\log x)^2$ is also known, but it requires more work, and the bound shown in the next theorem is good enough for our application in Corollary 10.6.

**Theorem 10.5.** *We have*

$$\pi_2(x) \ll \frac{x}{(\log x)^2} (\log\log x)^2.$$

**Proof.** We modify the proof given in Pollack's book [**299**, pp. 181–182]. We first define $\mathcal{A}$ and $\mathcal{P}$ as follows:

$$\begin{aligned} \mathcal{A} &= \{n(n+2) \mid n \le x\}, \\ \mathcal{P} &= \{p \mid p \text{ is a prime and } p \le z\}, \text{ and} \\ P &= \prod_{p\in\mathcal{P}} p. \end{aligned}$$

If both $n$ and $n+2$ are primes, then either $n \leq z$ or $n$ and $n+2$ are not divisible by any prime in $\mathcal{P}$. Therefore $\pi_2(x) \leq z + S(\mathcal{A}, \mathcal{P})$. Then we try to apply Brun's sieve to estimate $S(\mathcal{A}, \mathcal{P})$. To do that, we first need to determine appropriate choices for $X$ and $\alpha(d)$ to approximate $A_d = X\alpha(d) + r(d)$ for each $d \mid P$. Since $A_d$ is the number of $n \leq x$ such that $n(n+2) \equiv 0 \pmod{d}$, it is natural to define the following function:

$$v(d) = \#\{n \bmod d \mid n(n+2) \equiv 0 \ (\mathrm{mod}\ d)\}.$$

So each block of integers in $[1, d], (d, 2d], (2d, 3d], \ldots$ contains $v(d)$ solutions to $n(n+2) \equiv 0 \pmod{d}$. Therefore

$$\left\lfloor \frac{x}{d} \right\rfloor v(d) \leq A_d \leq \left(\left\lfloor \frac{x}{d} \right\rfloor + 1\right) v(d),$$

and so $A_d = \left\lfloor \frac{x}{d} \right\rfloor v(d) + \theta$ where $0 \leq \theta < v(d)$. So we take $X = x$, $\alpha(d) = \frac{v(d)}{d}$, $r(d) = \theta - \left\{\frac{x}{d}\right\} v(d)$, and therefore

$$A_d = \frac{x}{d} v(d) - \left\{\frac{x}{d}\right\} v(d) + \theta = X\alpha(d) + r(d).$$

Therefore $|r(d)| \leq v(d)$ and $\alpha(d)$ is multiplicative by the Chinese remainder theorem. Let $m = m(x)$ be an even positive integer to be determined later. For now, we let $x$ be large, $m = m(x) \to \infty$, and $z = z(x) \to \infty$ as $x \to \infty$. Therefore the main term for $S(\mathcal{A}, \mathcal{P})$ in Theorem 10.4 is

$$x \prod_{p \leq z} \left(1 - \frac{v(p)}{p}\right) = \frac{x}{2} \prod_{2 < p \leq z} \left(1 - \frac{v(p)}{p}\right) = \frac{x}{2} \prod_{2 < p \leq z} \left(1 - \frac{2}{p}\right)$$

$$= 2x \prod_{2 < p \leq z} \left(\frac{1 - \frac{2}{p}}{\left(1 - \frac{1}{p}\right)^2}\right) \prod_{p \leq z} \left(1 - \frac{1}{p}\right)^2. \tag{10.4}$$

By Mertens' theorem,

$$\prod_{p \leq z} \left(1 - \frac{1}{p}\right)^2 \sim \frac{e^{-2\gamma}}{(\log z)^2}.$$

We recall that $\prod_{n=1}^{\infty}(1 + |a_n|)$ converges if and only if $\sum_{n=1}^{\infty} |a_n|$ converges, and when the product converges, we also have

$$\prod_{x < n \leq y} (1 + |a_n|) \quad \text{converges to 1 as } x, y \to \infty.$$

From this, it is easy to verify that the first product in (10.4) converges to $C$ for some $C > 0$ as $z \to \infty$. Therefore

$$S(\mathcal{A}, \mathcal{P}) \sim \frac{2Ce^{-2\gamma}x}{(\log z)^2}.$$

Since $|r(d)| \leq v(d) \leq 2^{\omega(d)}$, the error term is $O(E_1 + E_2)$ where

$$E_1 = \sum_{\substack{d|P \\ \omega(d) \leq m}} 2^{\omega(d)} \text{ and } E_2 = x \sum_{\substack{d|P \\ \omega(d) \geq m}} \alpha(d).$$

So it is enough to show that $E_1$ and $E_2 \ll x/(\log z)^2$. We have

$$\begin{aligned}
E_1 &= \sum_{k=0}^{m} 2^k \binom{\pi(z)}{k} \leq \sum_{k=0}^{m} (2\pi(z))^k = (2\pi(z))^m \sum_{k=0}^{m} (2\pi(z))^{-k} \\
&\leq (2\pi(z))^m \sum_{k=0}^{\infty} (2\pi(z))^{-k} = (2\pi(z))^m \frac{1}{1 - \frac{1}{2\pi(z)}} \\
&\leq 2(2\pi(z))^m \leq 2z^m,
\end{aligned}$$

since $\pi(z) \leq z/2$ for large $x$. Next, we write

$$E_2 = x \sum_{k \geq m} \sum_{\substack{d|P \\ \omega(d)=k}} \alpha(d). \tag{10.5}$$

The inner sum in (10.5) is

$$\sum_{\substack{d|P \\ \omega(d)=k}} \alpha(d) = \sum_{p_1<p_2<\cdots<p_k \leq z} \alpha(p_1)\alpha(p_2)\cdots\alpha(p_k) \leq \frac{1}{k!}\left(\sum_{p \leq z} \alpha(p)\right)^k,$$

where the last inequality is obtained from the multinomial theorem as the expansion of $\left(\sum_{p \leq z} \alpha(p)\right)^k$ contains every term of the form $k!\, \alpha(p_1)\alpha(p_2)\cdots\alpha(p_k)$. By the fact that

$$\alpha(p) = v(p)/p \leq 2/p \text{ and } \sum_{p \leq z} 1/p \leq 2 \log\log z,$$

we obtain

$$\sum_{k \geq m} \frac{1}{k!}\left(\sum_{p \leq z} \alpha(p)\right)^k \leq \sum_{k \geq m} \frac{(4 \log\log z)^k}{k!}. \tag{10.6}$$

For each $k \geq m$, the ratio of the $(k+1)$th term to the $k$th in the right-hand side of (10.6) is

$$\frac{4\log\log z}{k+1} \leq \frac{4\log\log z}{m+1} \leq \frac{1}{2},$$

provided that $m+1 \geq 8\log\log z$. So suppose $m \geq 8\log\log z$. Then the right-hand side of (10.6) is bounded by twice its first term. Since $e^m = 1 + m + \frac{m^2}{2!} + \cdots \geq \frac{m^m}{m!}$, we have $m! \geq (m/e)^m$. Therefore the right-hand side of (10.6) is less than or equal to

$$\frac{2(4\log\log z)^m}{m!} \leq 2\left(\frac{4e\log\log z}{m}\right)^m \leq 2\left(\frac{1}{2}\right)^m,$$

provided that $m \geq 8e\log\log z$. Therefore, for such $m$, we have

$$E_2 \leq 2x(1/2)^m.$$

Combining the bounds for the main term, $E_1$, and $E_2$, we see that

$$S(\mathcal{A},\mathcal{P}) \ll \frac{x}{(\log z)^2} + z^m + \frac{x}{2^m}.$$

Let $z = x^{\frac{1}{48\log\log x}}$ and $m = 24\lfloor\log\log x\rfloor$. Then $z$ and $m$ satisfy all the conditions we use earlier, and so the above calculations are valid. In addition,

$$\frac{x}{(\log z)^2} \ll \frac{x}{(\log x)^2}(\log\log x)^2,\ z^m \ll x^{\frac{1}{2}},$$

and

$$\frac{x}{2^m} = \frac{x}{2^{24\lfloor\log\log x\rfloor}} \ll \frac{x}{2^{24\log\log x}} = \frac{x}{(\log x)^{24\log 2}} \leq \frac{x}{(\log x)^{11}}.$$

Therefore

$$S(\mathcal{A},\mathcal{P}) \ll \frac{x}{(\log x)^2}(\log\log x)^2.$$

Since $\pi_2(x) \leq z + S(\mathcal{A},\mathcal{P}) \ll S(\mathcal{A},\mathcal{P})$, we obtain the desired result. □

With the upper bound for $\pi_2(x)$ in the previous theorem, we can show that the reciprocal sum of twin primes is convergent.

**Corollary 10.6.** *We have*

$$\sum_{\substack{p\leq x\\ p \text{ and } p+2 \text{ are primes}}} \frac{1}{p} \quad \textit{converges as } x \to \infty.$$

**Proof.** The above sum is equal to

$$\begin{aligned}\int_{2^-}^{x} \frac{1}{t} d\pi_2(t) &= \frac{\pi_2(x)}{x} + \int_2^x \frac{\pi_2(t)}{t^2} dt \\ &\ll \frac{(\log\log x)^2}{(\log x)^2} + \int_2^x \frac{(\log\log t)^2}{t(\log t)^2} dt \\ &\ll 1 + \int_2^\infty \frac{1}{t(\log t)^{\frac{3}{2}}} dt \ll 1.\end{aligned}$$

This completes the proof. ☐

## 10.3. Selberg's Sieve

Another elementary sieve that is usually included in an introduction to sieve methods is the Selberg sieve, which, in many cases, is more powerful than Brun's sieve. To prove Selberg's sieve, we first recall the well-known Cauchy-Schwarz inequality as follows.

**Lemma 10.7.** (Cauchy-Schwarz inequality) *Let* $a_i, b_i \in \mathbb{R}$ *for all* $i = 1, 2, \dots, n$. *Then*

$$\left(\sum_{i=1}^n a_i b_i\right)^2 \le \left(\sum_{i=1}^n a_i^2\right)\left(\sum_{i=1}^n b_i^2\right). \tag{10.7}$$

*If* $a_i \neq 0$ *for some* $i$, *then* (10.7) *becomes an equality if and only if there exists* $t \in \mathbb{R}$ *such that* $b_i = ta_i$ *for all* $i = 1, 2, \dots, n$.

**Proof.** We have

$$\begin{aligned}0 \le \sum_{1\le i<j\le n} (a_i b_j - a_j b_i)^2 &= \sum_{1\le i<j\le n} (a_i^2 b_j^2 - 2a_i a_j b_i b_j + a_j^2 b_i^2) \\ &= \left(\sum_{i=1}^n a_i^2\right)\left(\sum_{j=1}^n b_j^2\right) - \left(\sum_{i=1}^n a_i b_i\right)^2,\end{aligned}$$

which implies (10.7). Furthermore, (10.7) becomes an equality if and only if $a_i b_j = a_j b_i$ for all $i \neq j$. So if $a_j \neq 0$ for some $j$, then we choose $t = b_j/a_j$ and obtain that $b_i = (b_j/a_j)a_i = ta_i$ for all $i = 1, 2, \dots, n$. ☐

Before giving a proof of Selberg's sieve, we also need the following lemma on the minimum value of a quadratic form.

**Lemma 10.8.** *Let $a_1, a_2, \dots, a_n$ be positive real numbers and let $b_1, b_2, \dots,$ $b_n$ be real numbers that are not all zero. Let $Q$ be a quadratic form given by*

$$Q(y_1, y_2, \dots, y_n) = \sum_{i=1}^{n} a_i y_i^2$$

*for all $y_1, y_2, \dots, y_n \in \mathbb{R}$ such that $\sum_{i=1}^{n} b_i y_i = 1$. Then the minimum value of $Q$ is*

$$m = \left( \sum_{i=1}^{n} (b_i^2/a_i) \right)^{-1}$$

*and this value is attained if and only if $y_i = mb_i/a_i$ for all $i = 1, 2, \dots, n$.*

**Proof.** Let $y_1, y_2, \dots, y_n$ satisfy $\sum_{i=1}^{n} b_i y_i$. By the Cauchy-Schwarz inequality, we have

$$1 = \left( \sum_{i=1}^{n} \left( \frac{b_i}{\sqrt{a_i}} \right) (\sqrt{a_i} y_i) \right)^2 \le \left( \sum_{i=1}^{n} \frac{b_i^2}{a_i} \right) \left( \sum_{i=1}^{n} a_i y_i^2 \right),$$

which implies $Q(y_1, y_2, \dots, y_n) \ge m$. In addition, $Q(y_1, y_2, \dots, y_n) = m$ if and only if there exists a real number $t$ such that

$$\sqrt{a_i} y_i = t b_i / \sqrt{a_i} \text{ for all } i,$$

or equivalently, $y_i = t b_i / a_i$ for all $i$. This implies that

$$1 = \sum_{i=1}^{n} b_i y_i = t \sum_{i=1}^{n} \frac{b_i^2}{a_i} = \frac{t}{m},$$

and so $t = m$ and $y_i = mb_i/a_i$ for all $i$. It is easy to check that if $y_i = mb_i/a_i$ for all $i$, then $\sum_{i=1}^{n} b_i y_i = 1$ and $Q(y_1, y_2, \dots, y_n) = m$. This completes the proof. ☐

We are now ready to prove Selberg's sieve. There are actually at least two versions of the Selberg sieve: the upper bound sieve and the lower bound sieve, but to keep things short and simple, we only focus on the upper bound sieve.

There are different versions of Selberg's upper bound sieve in the literature too; see for example, in the books by Cojocaru and Murty [**88**, pp. 119–124], Halberstam and Roth [**168**, pp. 208–224], Nathanson [**283**, pp. 180–191] and Montgomery and Vaughan [**273**, pp. 82–86]. Here we modify the proof of Selberg's sieve in a version given in [**283**, p. 180].

**Theorem 10.9.** (Selberg's Sieve) *Let* $\mathcal{A}$, $\mathcal{P}$, $P(z)$, $S(\mathcal{A},\mathcal{P},z)$, $A_d$ *be as before. Let* $g$ *be a multiplicative function such that* $0 < g(p) < 1$ *for all* $p \in \mathcal{P}$, *and let* $g_1$ *be a completely multiplicative function such that* $g_1(p) = g(p)$ *for all* $p \in \mathcal{P}$. *Let* $A_d = |\mathcal{A}|g(d) + r(d)$, *and*

$$G(z) = \sum_{\substack{m \le z \\ p|m \Rightarrow p \in \mathcal{P}}} g_1(m).$$

*Then*

$$S(\mathcal{A},\mathcal{P},z) \le \frac{|\mathcal{A}|}{G(z)} + \sum_{\substack{d \le z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)|.$$

**Proof.** Let $z \ge 2$. For each positive divisor $d$ of $P(z)$, let $\lambda(d)$ be a real number satisfying $\lambda(1) = 1$ and $\lambda(d) = 0$ for all $d \ge z$. Since

$$\left(\sum_{d|(a,P(z))} \lambda(d)\right)^2 \ge 0 \quad \text{and}$$

$$\left(\sum_{d|(a,P(z))} \lambda(d)\right)^2 = 1 \quad \text{if } (a,P(z)) = 1,$$

it follows that

$$\begin{aligned} S(\mathcal{A},\mathcal{P},z) &= \sum_{\substack{a \in \mathcal{A} \\ (a,P(z))=1}} 1 \le \sum_{a \in \mathcal{A}} \left(\sum_{d|(a,P(z))} \lambda(d)\right)^2 \\ &= \sum_{a \in \mathcal{A}} \sum_{\substack{d_1|a \\ d_1|P(z)}} \sum_{\substack{d_2|a \\ d_2|P(z)}} \lambda(d_1)\lambda(d_2) \\ &= \sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2) \sum_{\substack{a \in \mathcal{A} \\ [d_1,d_2]|\mathcal{A}}} 1. \end{aligned} \tag{10.8}$$

The innersum on the right-hand side of (10.8) is

$$A_{[d_1,d_2]} = |\mathcal{A}|g([d_1,d_2]) + r([d_1,d_2]).$$

In addition, since $g$ is multiplicative, it is not difficult to verify that $g([d_1,d_2])g((d_1,d_2)) = g(d_1)g(d_2)$ for all $d_1, d_2 \in \mathbb{N}$. Furthermore, we have $\lambda(d) = 0$ for $d \geq z$. After the calculation of the right-hand side of (10.8), we therefore obtain that

$$S(\mathcal{A}, \mathcal{P}, z) \leq |\mathcal{A}|Q + R, \tag{10.9}$$

where

$$Q = \sum_{\substack{d_1, d_2 < z \\ d_1, d_2 | P(z)}} \frac{1}{g((d_1, d_2))} g(d_1)\lambda(d_1)g(d_2)\lambda(d_2), \quad \text{and}$$

$$R = \sum_{\substack{d_1, d_2 < z \\ d_1, d_2 | P(z)}} \lambda(d_1)\lambda(d_2)r([d_1, d_2]).$$

Let $\mathcal{D} = \{d \in \mathbb{N} \mid d \text{ divides } P(z) \text{ and } d < z\}$. Then $\mathcal{D}$ is a divisor-closed set of squarefree integers, that is, if $n \in \mathcal{D}$ and $d \mid n$, then $d \in \mathcal{D}$ too. Since $0 < g(p) < 1$ for all $p \in \mathcal{P}$, we see that for each $n \in \mathcal{D}$ and the divisor $d$ of $n$, we have

$$0 < g(n) \leq 1, \ (d, n/d) = 1, \ \text{and } g(n) = g(d)g(n/d).$$

For each $n \in \mathbb{N}$, we define $f(n) = \left(\mu * \frac{1}{g}\right)(n)$, or equivalently,

$$f(n) = \sum_{d|n} \frac{\mu(d)}{g(n/d)} = \frac{1}{g(n)} \sum_{d|n} \mu(d)g(d) = \frac{1}{g(n)} \prod_{p|n} (1 - g(p)). \tag{10.10}$$

Then $f(n) > 0$ and $f(n_1 n_2) = f(n_1)f(n_2)$ if $(n_1, n_2) = 1$. By the Möbius inversion formula, $\frac{1}{g} = f * 1$. Therefore

$$\begin{aligned} Q &= \sum_{d_1, d_2 \in \mathcal{D}} \frac{1}{g((d_1, d_2))} g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) \\ &= \sum_{d_1, d_2 \in \mathcal{D}} \sum_{d|d_1, d|d_2} f(d)g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) \\ &= \sum_{d \in \mathcal{D}} f(d) \sum_{\substack{d_1, d_2 \in \mathcal{D} \\ d|d_1, d|d_2}} g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) \\ &= \sum_{k \in \mathcal{D}} f(k) \left( \sum_{\substack{d \in \mathcal{D} \\ k|d}} g(d)\lambda(d) \right)^2 = \sum_{k \in \mathcal{D}} f(k) y_k^2, \end{aligned}$$

where $y_k = \sum_{d \in \mathcal{D}, k|d} g(d)\lambda(d)$. Therefore $Q$ is a quadratic form in the variables $y_k$. Since $\mathcal{D}$ is finite and divisor-closed, we can apply another version of the Möbius inversion formula to obtain

$$g(d)\lambda(d) = \sum_{\substack{k\in\mathcal{D}\\ d|k}} \mu\left(\frac{k}{d}\right) y_k = \mu(d) \sum_{\substack{k\in\mathcal{D}\\ d|k}} \mu(k) y_k. \tag{10.11}$$

In particular, if $d = 1$, then $\sum_{k\in\mathcal{D}} \mu(k)y_k = 1$. So $Q$ is in the form suitable for the application of Lemma 10.8. Let

$$F(z) = \sum_{k\in\mathcal{D}} \frac{1}{f(k)}.$$

By applying Lemma 10.8 with $a_k = f(k)$ and $b_k = \mu(k)$, we see that the minimum value of $Q$ is

$$\left(\sum_{k\in\mathcal{D}} \frac{\mu(k)^2}{f(k)}\right)^{-1} = \left(\sum_{k\in\mathcal{D}} \frac{1}{f(k)}\right)^{-1} = \frac{1}{F(z)},$$

and this minimum is attained when

$$y_k = \frac{\mu(k)}{F(z)f(k)}. \tag{10.12}$$

By (10.11), we obtain

$$\lambda(d) = \frac{\mu(d)}{g(d)} \sum_{\substack{k\in\mathcal{D}\\ d|k}} \mu(k) y_k = \frac{\mu(d)}{g(d)} \sum_{\substack{d\ell<z\\ d\ell|P(z)}} \mu(d\ell) y_{d\ell}. \tag{10.13}$$

Since $P(z)$ is squarefree, we see that $d$, $\ell$ in the above sum are relatively prime. Substituting $y_k$ from (10.12) in (10.13), we obtain

$$\begin{aligned}\lambda(d) &= \frac{\mu(d)}{g(d)} \sum_{\substack{\ell<z/d\\ d\ell|P(z)}} \frac{\mu^2(d\ell)}{F(z)f(d\ell)} \\ &= \frac{\mu(d)}{f(d)g(d)F(z)} \sum_{\substack{\ell<z/d\\ d\ell|P(z)}} \frac{1}{f(\ell)} = \frac{\mu(d)F_d(z)}{f(d)g(d)F(z)}, \qquad (10.14)\end{aligned}$$

where

$$F_d(z) = \sum_{\substack{\ell<z/d\\ d\ell|P(z)}} \frac{1}{f(\ell)}.$$

Let $d$ be any positive divisor of $P(z)$. Then

$$F(z) = \sum_{k\in\mathcal{D}} (f(k))^{-1} = \sum_{\ell|d} \sum_{\substack{k\in\mathcal{D}\\ (k,d)=\ell}} (f(k))^{-1} = \sum_{\ell|d} \sum_{\substack{\ell m<z\\ \ell m|P(z)\\ (\ell m,d)=\ell}} (f(\ell m))^{-1}.$$

Again $\ell, m$ in the above sum are relatively prime, so

$$\begin{aligned}F(z) &= \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell\\ \ell m|P(z)\\ (m,d/\ell)=1}} \frac{1}{f(m)} = \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell\\ m|P(z)\\ (m,d)=1}} \frac{1}{f(m)}\\ &= \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell\\ dm|P(z)}} \frac{1}{f(m)} \geq \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/d\\ dm|P(z)}} \frac{1}{f(m)}\\ &= F_d(z) \sum_{\ell|d} \frac{1}{f(\ell)} = \frac{F_d(z)}{f(d)} \sum_{\ell|d} f\left(\frac{d}{\ell}\right) = \frac{F_d(z)}{f(d)g(d)}. \qquad (10.15)\end{aligned}$$

By (10.14) and (10.15), we see that $|\lambda(d)| \leq 1$. In addition, if $d \in \mathbb{N}$ is squarefree, then there are exactly $3^{\omega(d)}$ ordered pairs of positive integers $d_1, d_2$ such that $[d_1, d_2] = d$. Moreover, if $d_1, d_2 < z$, then $d = [d_1, d_2] < z^2$. Furthermore, if $d_1, d_2 \mid P(z)$, then $d = [d_1, d_2]$ divides $P(z)$ and is squarefree. Therefore

$$|R| \leq \sum_{\substack{d_1,d_2<z\\ d_1,d_2|P(z)}} |r([d_1, d_2])| \leq \sum_{\substack{d<z^2\\ d|P(z)}} 3^{\omega(d)}|r(d)|. \qquad (10.16)$$

We recall that the minimum value of $Q$ is $(F(z))^{-1}$. By substituting the minimum value of $Q$ in (10.9) and applying (10.16), we obtain

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{|\mathcal{A}|}{F(z)} + \sum_{\substack{d<z^2\\ d|P(z)}} 3^{\omega(d)}|r(d)|.$$

So it remains to show that $F(z) \geq G(z)$. By (10.10) and the definitions of $F(z)$, $g_1$, and $g$, we have

$$F(z) = \sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} (1 - g_1(p))^{-1} = \sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} \sum_{r=0}^{\infty} g_1(p^r).$$

Then

$$\begin{aligned} F(z) &= \sum_{k\in\mathcal{D}} g_1(k) \sum_{\substack{\ell=1\\ p|\ell\Rightarrow p|k}}^{\infty} g_1(\ell) = \sum_{k\in\mathcal{D}} \sum_{\substack{\ell=1\\ p|\ell\Rightarrow p|k}}^{\infty} g_1(k\ell) \\ &= \sum_{k\in\mathcal{D}} \sum_{\substack{m=1\\ k|m\\ p|(m/k)\Rightarrow p|k}}^{\infty} g_1(m) = \sum_{m=1}^{\infty} g_1(m) \sum_{\substack{k\in\mathcal{D}\\ k|m\\ p|(m/k)\Rightarrow p|k}} 1 \\ &\geq \sum_{\substack{m<z\\ p|m\Rightarrow p\in\mathcal{P}}} g_1(m) \sum_{\substack{k\in\mathcal{D}\\ k|m\\ p|(m/k)\Rightarrow p|k}} 1. \end{aligned}$$

Since we can choose $k$ to be the product of the distinct primes dividing $m$, we see that the above innersum is at least 1. Therefore

$$F(z) \geq \sum_{\substack{m<z\\ p|m\Rightarrow p\in\mathcal{P}}} g_1(m) = G(z).$$

This completes the proof. □

Another version of Selberg's sieve that looks slightly different from Theorem 10.9 is given in Cojocaru and Murty [**88**, pp. 119–124]. An axiomatic formulation of the higher rank version of the Selberg sieve also appears in the work of Vatwani [**420**], and Ram Murty and Vatwani [**335**]. There are many applications of sieve methods given in Cojocaru and Murty [**88**], Pollack [**299**], Nathanson [**283**], and Montgomery and Vaughan [**273**] too. Here we mention only $r(N)$, the number of ordered representations of $N$ as a sum of two primes since we will use it again in Section 10.5.

**Theorem 10.10.** *Let $N$ be an even positive integer, and let $r(N)$ denote the number of representations of $N$ as the sum of two primes. Then*

$$r(N) \ll \frac{N}{(\log N)^2} \prod_{p|N} \left(1 + \frac{1}{p}\right),$$

*where the implied constant is absolute.*

**Proof.** Let $N$ be a large even positive integer. Then $r(N)$ counts the number of primes $p < N$ such that $N - p$ is also prime. Let $\mathcal{P}$ be the set of all primes, $a_n = n(N-n)$, $\mathcal{A} = \{a_n \mid 1 \leq n \leq N\}$, and $2 < z \leq \sqrt{N}$. If

$\sqrt{N} < n < N-\sqrt{N}$ and both $n$ and $N-n$ are prime, then $a_n \not\equiv 0 \pmod{p}$ for any $p \le z$, and so $a_n$ is counted in $S(\mathcal{A}, \mathcal{P}, z)$. Since

$$r(N) \le \sum_{n\le\sqrt{N}} 1 + \sum_{\substack{\sqrt{N}<n<N-\sqrt{N} \\ n \text{ and } N-n \text{ are prime}}} 1 + \sum_{N-\sqrt{n}\le n<N} 1,$$

we obtain

$$r(N) \le 2\sqrt{N} + S(\mathcal{A}, \mathcal{P}, z).$$

We will use Selberg's sieve to obtain an upper bound for $S(\mathcal{A}, \mathcal{P}, z)$ and we will also use the same notation as in Theorem 10.9. We need to find $A_d$ and write it in the form $A_d = |\mathcal{A}|g(d) + r(d)$. Let $d \mid P(z)$. We recall that $A_d$ is the number of $n \le N$ such that $a_n \equiv 0 \pmod{d}$, and $a_n \equiv 0 \pmod{d}$ if and only if $a_n \equiv 0 \pmod{p}$ for every prime $p$ dividing $d$. In addition, for each prime $p$, we have $a_n \equiv 0 \pmod{p}$ if and only if

$$n \equiv 0 \pmod{p} \quad \text{or} \quad n \equiv N \pmod{p}. \tag{10.17}$$

If $p \mid N$, then both congruences in (10.17) are the same; if $p \nmid N$, then they are different. Let $d = p_1p_2\cdots p_kq_1q_2\cdots q_\ell$ where the primes $p_i$ divide $N$ and the primes $q_j$ do not divide $N$. Since

$$A_d = \sum_{\substack{n\le N \\ a_n\equiv 0 \pmod{d}}} 1 = \sum_{\substack{n\le N \\ n\equiv 0 \pmod{p_i} \text{ for all } i \\ n\equiv 0,N \pmod{q_j} \text{ for all } j}} 1,$$

we need to count the number of solutions to the system of congruences

$$n \equiv 0 \pmod{p_i} \text{ for each } i = 1, 2, \ldots, k \text{ and}$$
$$n \equiv 0, N \pmod{q_j} \text{ for each } j = 1, 2, \ldots, \ell.$$

By the Chinese remainder theorem, there are $2^\ell$ solutions modulo $d$, say $b_1, b_2, \ldots, b_{2^\ell}$. Therefore

$$A_d = \sum_{\substack{n\le N \\ n\equiv b_1,b_2,\ldots,b_{2^\ell} \pmod{d}}} 1 = 2^\ell\frac{N}{d} + r(d) \tag{10.18}$$

where $|r(d)| \le 2^\ell \le 2^{\omega(d)}$. From (10.18), we should define a function g so that $g(d) = \frac{2^\ell}{d}$. Let g be a completely multiplicative function defined by

$$g(p) = \begin{cases} 1/p & \text{if } p \text{ divides } N; \\ 2/p & \text{if } p \text{ does not divide } N. \end{cases}$$

Then $g_1(m) = g(m)$ for all $m \in \mathbb{N}$, $0 < g(p) < 1$ for all primes $p$, $g(d) = 2^\ell/d$, and (10.18) becomes

$$A_d = |\mathcal{A}|g(d) + r(d) \quad \text{with} \quad |r(d)| \leq 2^{\omega(d)}.$$

Next, we calculate $G(z) = \sum_{m \leq z} g(m)$. We remark that the primes $p_i$ and $q_j$ in the factorization of $d$ are used to explain the calculation of $A_d$, which is already finished. So in the following calculation, we use the notation $p_i$, $q_j$ again, but they are not necessarily the same prime numbers. For $1 < m \leq z$, we see that $m$ is divisible by some prime $p \mid P(z)$, so we write

$$m = \prod_{i=1}^{k} p_i^{r_i} \prod_{j=1}^{\ell} q_j^{s_j},$$

where $p_i \mid N$, $q_j \nmid N$ for each $i, j$. Then

$$g(m) = \prod_{i=1}^{k} \left(\frac{1}{p_i}\right)^{r_i} \prod_{j=1}^{\ell} \left(\frac{2}{q_j}\right)^{s_i} = \frac{2^{s_1+s_2+\cdots+s_\ell}}{m}.$$

Let $d_N(m)$ be the number of positive divisors of $m$ that are relatively prime to $N$. Then

$$d_N(m) = d\left(\prod_{j=1}^{\ell} q_j^{s_i}\right) = \prod_{j=1}^{\ell}(s_j + 1) \leq \prod_{j=1}^{\ell} 2^{s_j}.$$

Therefore

$$g(m) \geq \frac{d_N(m)}{m} \quad \text{and} \quad G(z) \geq \sum_{m \leq z} \frac{d_N(m)}{m}.$$

Since

$$\prod_{p \mid N} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{\substack{t=1 \\ p \mid t \Rightarrow p \mid N}}^{\infty} \frac{1}{t},$$

we obtain that

$$\begin{aligned}\prod_{p\mid N}\left(1-\frac{1}{p}\right)^{-1}G(z) &\geq \sum_{m\leq z}\frac{d_N(m)}{m}\sum_{\substack{t=1\\ p\mid t\Rightarrow p\mid N}}^{\infty}\frac{1}{t}\\ &= \sum_{m\leq z}d_N(m)\sum_{\substack{t=1\\ p\mid t\Rightarrow p\mid N}}^{\infty}\frac{1}{mt}\\ &= \sum_{m\leq z}d_N(m)\sum_{\substack{w=1\\ m\mid w\\ p\mid (w/m)\Rightarrow p\mid N}}^{\infty}\frac{1}{w}\\ &= \sum_{w=1}^{\infty}\frac{1}{w}\sum_{\substack{m\leq z\\ m\mid w\\ p\mid (w/m)\Rightarrow p\mid N}}d_N(m)\\ &\geq \sum_{w\leq z}\frac{1}{w}\sum_{\substack{m\mid w\\ p\mid (w/m)\Rightarrow p\mid N}}d_N(m). \qquad (10.19)\end{aligned}$$

For each $w \leq z$, write $w = \prod_{i=1}^{k} p_i^{u_i}\prod_{j=1}^{\ell} q_j^{v_j}$ where $p_i \mid N$ and $q_j \nmid N$ for each $i, j$. Since $m$ in the above sum divides $w$, we obtain $0 \leq r_i \leq u_i$ and $0 \leq s_j \leq v_j$ for all $i, j$. Since every prime dividing $w/m$ is a prime divisor of $N$, we must have $s_j = v_j$ for all $j$. Therefore

$$m = \left(\prod_{i=1}^{k} p_i^{r_i}\right)\left(\prod_{j=1}^{\ell} q_j^{v_j}\right) \quad \text{and} \quad d_N(m) = \prod_{j=1}^{\ell}(v_j+1).$$

For each $w \leq z$, we have

$$\begin{aligned}\sum_{\substack{m\mid w\\ p\mid (w/m)\Rightarrow p\mid N}}d_N(m) &= \prod_{j=1}^{\ell}(v_j+1)\sum_{\substack{m\mid w\\ p\mid (w/m)\Rightarrow p\mid N}}1\\ &= \prod_{j=1}^{\ell}(v_j+1)\prod_{i=1}^{k}(u_i+1) = d(w).\end{aligned}$$

Therefore (10.19) implies that

$$\prod_{p\mid N}\left(1-\frac{1}{p}\right)^{-1}G(z) \geq \sum_{w\leq z}\frac{d(w)}{w} \gg (\log z)^2.$$

Then

$$\begin{aligned}\frac{|\mathcal{A}|}{G(z)} &\ll \frac{N}{(\log z)^2}\prod_{p|N}\left(1-\frac{1}{p}\right)^{-1}\\ &= \frac{N}{(\log z)^2}\prod_{p|N}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p|N}\left(1+\frac{1}{p}\right)\\ &\ll \frac{N}{(\log z)^2}\prod_{p|N}\left(1+\frac{1}{p}\right),\end{aligned}$$

where the last estimate follows from the fact that the infinite product $\prod_p(1-p^{-2})^{-1}$ converges. By Selberg's sieve, we obtain

$$S(\mathcal{A},\mathcal{P},z) \le \frac{|\mathcal{A}|}{G(z)} + \sum_{\substack{d\le z^2\\ d|P(z)}} 3^{\omega(d)}|r(d)| \ll \frac{N}{(\log z)^2}\prod_{p|N}\left(1+\frac{1}{p}\right) + R,$$

where

$$R = \sum_{\substack{d\le z^2\\ d|P(z)}} 3^{\omega(d)}|r(d)| = \sum_{\substack{d\le z^2\\ d|P(z)}} 6^{\omega(d)} \le \sum_{d\le z^2} 6^{\omega(d)}.$$

For $d \le z^2$, we have

$$6^{\omega(d)} = \left(2^{\omega(d)}\right)^{\frac{\log 6}{\log 2}} \le d^{\frac{\log 6}{\log 2}} \le z^{\frac{2\log 6}{\log 2}}.$$

Therefore $R \le z^{2+(2\log 6/\log 2)} \le z^{7.2}$. Hence

$$S(\mathcal{A},\mathcal{P},z) \ll \frac{N}{(\log z)^2}\prod_{p|N}\left(1+\frac{1}{p}\right) + z^{7.2}. \tag{10.20}$$

Now we have to choose $z \le \sqrt{N}$ so that the above estimate leads to the desired result. Considering $z = N^{\theta}$ where $\theta < \frac{1}{2}$ and $z^{7.2} < N$, we see that we should take $z = N^{\frac{1}{8}}$. Then (10.20) leads to the desired result. This completes the proof. ☐

## 10.4. Introduction to Additive Number Theory

Additive number theory and the study of sumsets have a long history, dating back at least to Lagrange in 1770, who proved that every natural number can be written as a sum of four squares of integers. In 1813, Cauchy gave a lower bound for the cardinality of the sumset $A+B$ where $A$ and $B$ are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$. Davenport [**97**] rediscovered Cauchy's result in 1935, and it is now known as the Cauchy-Davenport theorem. Since then, sumsets have been investigated by many other mathematicians. For additional information, we refer the reader to the books by Freiman [**132**], Halberstam and Roth [**168**], Nathanson [**281**, **283**], Tao and Vu [**397**], and Vaughan [**422**].

Before proceeding further, let us introduce some notations and terminologies that are used throughout this section. Let $A$ and $B$ be nonempty subsets of $\mathbb{Z}$, $h \in \mathbb{N}$, and $x \in \mathbb{Z}$. The sumset $A + B$, the $h$-fold sumset $hA$, the translation $x + A$, and the dilation $x * A$ are defined by

$$\begin{aligned} A + B &= \{a + b \mid a \in A \text{ and } b \in B\}, \\ hA &= \{a_1 + a_2 + \cdots + a_h \mid a_i \in A \text{ for all } i\}, \\ x + A &= A + x = \{a + x \mid a \in A\}, \text{ and} \\ x * A &= A * x = \{ax \mid a \in A\}. \end{aligned}$$

In addition, if $A_1, A_2, \ldots, A_h$ are nonempty sets of integers, then

$$\begin{aligned} &A_1 + A_2 + \cdots + A_h = \\ &\quad \{a_1 + a_2 + \cdots + a_h \mid \; a_i \in A_i \text{ for every } i = 1, 2, \ldots, h\}. \end{aligned}$$

The study of sumsets may be extended from subsets of $\mathbb{Z}$ to any abelian groups, but for our purpose, we focus only on subsets of $\mathbb{N}_0$. So let $A \subseteq \mathbb{N}_0$.

We say that $A$ is an additive basis of order $h$ if every positive integer can be written as a sum of $h$ elements of $A$, and that $A$ is an asymptotic additive basis of order $h$ if every sufficiently large positive integer is a sum of $h$ members of $A$, that is, there exists $n \in \mathbb{N}$ such that $\mathbb{Z} \cap [n, \infty)$ is a subset of $hA$. Since we only focus on the addition, we usually drop the words additive and simply say that $A$ is a basis or an asymptotic basis. In addition, we call $A$ a basis (or asymptotic basis) of finite order if $A$ is a basis (or asymptotic basis) of order $h$ for some $h \in \mathbb{N}$.

A central problem in additive number theory is to determine whether a given set $A$ is a basis (or an asymptotic basis) of finite order, and if it is, we would also like to know the smallest $h \in \mathbb{N}$ such that $hA$ contains every positive integer (or every sufficiently large positive integer). Furthermore, if the smallest $h \in \mathbb{N}$ is found, then it may also be desirable to explicitly obtain the smallest positive integer $n$ such that $\mathbb{Z} \cap [n, \infty)$ is a subset of $hA$. In addition, if such an $h$ is found, it may be of interest to describe the structure of $(h-1)A$ or $h_1A$ where $h_1$ is a positive integer less than but close to $h$. Finally, if $h$ and $n$ are like the smallest integers described above, then we say that $A$ is a basis (or asymptotic basis) of exact order $h$, and that $n-1$, the largest integer that is not the element of the cofinite set $hA$, the Frobenius number of $hA$.

Let us give one more set of terminologies about the density of sequences of integers. Let $A$ be a set (or a sequence) of nonnegative integers and $A(x)$ is the number of elements in $A \cap [1, x]$. Then the natural asymptotic density $D(A)$, upper asymptotic density $\overline{D}(A)$, and lower asymptotic density $\underline{D}(A)$ of $A$ are defined by

$$D(A) = \lim_{x\to\infty} \frac{A(x)}{x}, \overline{D}(A) = \limsup_{x\to\infty} \frac{A(x)}{x}, \underline{D}(A) = \liminf_{x\to\infty} \frac{A(x)}{x}.$$

We often call $D(A)$, $\overline{D}(A)$, and $\underline{D}(A)$ by shorter names such as the natural density, the upper density, and the lower density, respectively.

Next we give various examples to illustrate the idea of being a basis.

**Example 10.11.** (Not every set can be a basis even though it has a positive natural density) Let $A = \{n \in \mathbb{N}_0 \mid n \equiv 0 \pmod 2\}$. Then $D(A) = 1/2$ but no odd integer is a sum of elements of $A$. In fact, $hA = A$ for all $h \in \mathbb{N}$. More generally, if $(a, m) > 1$, then the set $A$ of nonnegative integers that are congruent to $a$ mod $m$ cannot be a basis because any integer coprime to $m$ is not a sum of elements in $A$.

**Example 10.12.** (A basis of infinite order, the number of summands is not restricted) Let $A = \{2^k \mid k \in \mathbb{N}_0\}$. Then it is well known that every positive integer is a sum of elements of $A$. However, $A$ is not a basis of finite order since there is no $h \in \mathbb{N}$ such that $hA$ contains $\mathbb{N}$. For example, $2^k - 1 = 1 + 2 + 2^2 + \cdots + 2^{k-1}$ is the most economical way to write $2^k - 1$ as a sum of elements in $A$ (in the sense that if we write $2^k - 1$ as a sum of elements of $A$ in the other ways, then the number of summands is larger than $k$).

Therefore if $k > h$, then $2^k - 1 \notin hA$. Perhaps, we can call $A$ a basis of infinite order. However, being a basis of infinite order is not generally interesting or at least, it is not our interest in this chapter. For instance, if $1 \in A$, then $A$ can always be considered as a basis of infinite order, because we can always write $n = 1 + 1 + \cdots + 1$ for any $n \in \mathbb{N}$. For this kind of problem, it is more interesting to count the number of representations of each $n \in \mathbb{N}$ as a sum of elements in $A$.

For example, if $A = \mathbb{N}$ and we would like to count the number of (ordered or unordered) representations of each $n \in \mathbb{N}$ as a sum of elements in $A$, then these are the composition and partition problems. Nevertheless, to keep the book simple and not too long, we skip this and other related problems. The interested reader can find more information on compositions, partitions, and related topics in, for instance, the books by Andrews [**11**] and Stanley [**381**, **382**].

**Remark 10.13.** (Being a basis vs having positive natural density) From Examples 10.11 and 10.12, we see that arithmetic progressions, although they have positive natural density, are bad for sumsets because they may not be a basis. In fact, it is not difficult to prove that every arithmetic progression $a \pmod{m}$ with $m \geq 2$ is not an asymptotic basis of finite order. Furthermore, if $(a, m) > 1$, then it is not even an asymptotic basis of infinite order.

While geometric progressions are very sparse, some of them can at least be a basis of infinite order. We may also say that the positivity of the natural asymptotic density of $A$ generally has nothing to do with $A$ being a basis. However, we show in the next section that if $0 \in A$ and the Schnirelmann density of $A$ is positive, then $A$ is a basis of finite order.

From this point on, we focus only on bases of finite order. So if $A$ is a basis of finite order, we often simply say $A$ is a basis, and the same applies to an asymptotic basis.

**Example 10.14.** (Squares, order, and exact order) Let $A$ be the set of all squares of nonnegative integers. Then Lagrange's theorem states that $4A = \mathbb{N}_0$. Gauss and Legendre also showed that $n \in 3A$ if and only if $n$ is not of the form $4^a(8b + 7)$ for any integers $a, b \geq 0$. So $A$ is a basis of order 4 but not order 3. In other words, $A$ is a basis of exact order 4. The structure of $2A$ is also well known, that is, $2A$ consisting of 0, 1, and the integers $n > 1$ of the form $n = \prod_{p^a \| n} p^a$ where $a$ is even for all primes $p \equiv 3 \pmod{4}$. Therefore the structure of the sumsets $4A$, $3A$, $2A$ are completely solved.

**Example 10.15.** (Classical Waring's problem) For each integer $k \geq 2$, let $A = A_k = \{n^k \mid n \in \mathbb{N}_0\}$ be the set of all $k$th powers of nonnegative integers, and let $h = g(k)$ be the smallest positive integer such that $hA$ contains $\mathbb{N}_0$. Waring stated that every number is a sum of four squares; every number is a sum of nine cubes; every number is a sum of 19 fourth powers of nonnegative integers, and so on. It is presumed that by this, Waring meant that for every $k \geq 2$, the integer $h = g(k)$ exists and that it satisfies $g(2) = 4$, $g(3) = 9$, $g(4) = 19$, and so on. Langrange proved that $g(2) = 4$, but by the end of the nineteenth century, the existence of $g(k)$ was known for only a finite number of $k \leq 10$. However, Hilbert in 1909 showed that $g(k)$ indeed exists for every $k$. As of 2022, we have an almost complete solution to this problem. We recall that $\lfloor x \rfloor$ is the largest integer not exceeding $x$, and $\{x\} = x - \lfloor x \rfloor$. In addition, let

$$a(k) = 2^k \left\{ \left(\frac{3}{2}\right)^k \right\} + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor \text{ and}$$

$$b(k) = \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor.$$

As the result of the work of many mathematicians, we know that

$$g(k) = \begin{cases} 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2, & \text{if } a(k) \leq 2^k; \\ 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor - 2, & \text{if } a(k) > 2^k \text{ and } b(k) = 2^k; \\ 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor - 3, & \text{if } a(k) > 2^k \text{ and } b(k) > 2^k. \end{cases}$$

Kubina and Wunderlich [**233**] showed that $a(k) \leq 2^k$ for all $k \leq 4716 \times 10^5$, and Mahler [**256**] proved that $a(k) > 2^k$ for at most a finite number of $k$ (but those exceptional $k$, if they exist, cannot be specified). As of 2022, the value of $k$ for which $a(k) > 2^k$ is not known. So it is conjectured that this never happens, that is, $a(k) \leq 2^k$ and $g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$ for all $k \geq 1$.

**Example 10.16.** (Modern Waring's problem) By the discussion in Example 10.15, we know that the set $A = A_k$ is a basis of exact order $g(k)$ for every $k$ and that the value of $g(k)$ is known for all except a finite number of $k$.

Since $A$ is a basis, it is also an asymptotic basis. However, the exact order of $A$ as an asymptotic basis is not necessarily $g(k)$. The modern version of Waring's problem is to determine the smallest positive integer $h = G(k)$ such that $hA$ contains all sufficiently large positive integers. This version is much more difficult and it is still very much open: the values of $G(k)$ are known only for $k = 2$ and $k = 4$, namely, $G(2) = 4$ and $G(4) = 16$.

What is known about $G(k)$ has been obtained by using the Hardy-Littlewood circle method, which has its genesis in the celebrated paper of Hardy and Ramanujan [**177**] on the partition function. We give an outline of the use of the circle method in Waring's problem in the next section. For many more details about this, we refer the reader to the survey article by Vaughan and Wooley [**426**], and the books by Davenport [**99**] and Vaughan [**422**].

**Example 10.17.** (Basis vs asymptotic basis) Although every basis $A \subseteq \mathbb{N}_0$ is an asymptotic basis, the corresponding questions of determining the smallest positive integer $h$ such that $hA = \mathbb{N}_0$ or $hA$ contains all sufficiently large integers may be totally different. As in Waring's problem, the value of $h = g(k)$ is known for all except a finite number of $k$ while $h = G(k)$ is known only for $k = 2$ and $k = 4$. Therefore being a basis and being an asymptotic basis may be similar but the calculations for the exact order of a set $A$ as a basis or as an asymptotic basis are generally a different problem.

**Example 10.18.** (The importance of zero in a basis) In some situations, the inclusion or exclusion of zero as an element of $A$ may lead to a totally different problem. For example, if $A$ is the set of all squares of integers (including zero) as in Example 10.14, the structure of $3A$ is completely known; however, the structure of $3(A\backslash\{0\})$ is still open, and only a partial answer is known, based on the generalized Riemann hypothesis [**147**, **162**, **222**]. The zero is also important in the application of Schnirelmann's and Mann's theorems as shown in Example 10.27 in the next section.

**Example 10.19.** (The importance of 1 in a basis) It is easy to see that if $A \subseteq \mathbb{N}_0$ and $1 \notin A$, then $A$ cannot be a basis since $1 \notin hA$ for any $h \in A$. Nevertheless, such a set $A$ may be an asymptotic basis. However, in order to apply the Schnirelmann basis theorem to a set $A$, it is necessary that $1 \in A$. We give more details about this in Example 10.28 in the next section.

**Example 10.20.** (Basis, asymptotic basis, zero, and one) If $A \subseteq \mathbb{N}_0$ and both 0 and 1 are in $A$, then $A$ is a basis if and only if $A$ is an asymptotic basis. So this example is another illustration of the importance of zero and one in a basis or an asymptotic basis. To verify this, suppose $A$ is an asymptotic basis. So there are positive integers $h$ and $N$ such that $hA$

contains $\mathbb{Z} \cap [N, \infty)$. Since $0, 1 \in A$, we can write all the integers $n \leq N$ as a sum of $N$ elements in $A$, namely,

$$n = 1 + 1 + \cdots + 1 + 0 + 0 + \cdots + 0,$$

where the number of 1's and 0's are $n$ and $N - n$. Let $h_1 = \max\{h, N\}$. Then every integer in $\mathbb{N}_0$ can be written as a sum of $h_1$ elements of $A$, that is $h_1 A = \mathbb{N}_0$. So $A$ is a basis. The other direction is obvious. So the verification is complete.

We end this section by summarizing some fundamental questions in additive number theory. The universal set $X$ in questions may be $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Z}^n$, or any additive abelian group, but if there is anything confusing or ambiguous, the reader can always consider $X = \mathbb{N}_0$.

1. Given sets $A$ and $B$, describe the sumset $A + B$.
2. Given set $A$, describe the $h$-fold sumset $hA$. Is $A$ a basis? Is $A$ an asymptotic basis? If $A \subseteq \mathbb{N}_0$ is a basis, what is the smallest $h \in \mathbb{N}$ such that $hA = \mathbb{N}_0$?
3. Suppose $A$ is an asymptotic basis. What is the smallest $h \in \mathbb{N}$ such that $hA$ is cofinite? If $A \subseteq \mathbb{N}_0$ and such an $h$ is found, what is the smallest integer $n$ such that $hA$ contains $\mathbb{Z} \cap [n, \infty)$? If such an $h$ is found, can we also determine the structure of $h_1 A$ where $h_1$ is close to $h$.
4. Given a set $C$, are there sets $A$ and $B$ satisfying some specified conditions such that $A + B = C$? Are there large sets $A$ and $B$ such that the symmetric difference $(A + B)\Delta C$ is small? Here $A\Delta B = (A - B) \cup (B - A)$. The words large set and small set do not have a rigorous mathematical meaning, but there are some mathematical measures that we can select. For example, if the sets in the question are infinite, we may like to see the sets $A$, $B$ such that

   $$\limsup_{x\to\infty} \frac{A(x)}{C(x)} \text{ and } \limsup_{x\to\infty} \frac{B(x)}{C(x)} \text{ are positive.}$$

   The small sets can be a finite set or that

   $$\liminf_{x\to\infty} \frac{((A + B)\Delta C)(x)}{C(x)} = 0.$$

   We should emphasize that this is just an example of how to measure small or large sets, but there are some situations where one measure seems more natural than another measure; there are also some situations where different measures seem to be equally interesting.

5. Given sets $A$ and $C$, does there exist a set $B$ satisfying some specified conditions such that $A + B = C$, $A + B \subseteq C$, or $(A + B)\Delta C$ is small?
6. If $x \in A + B$, describe the function that counts the number of (ordered or unordered) representations of $x$ as a sum of an element of $A$ and an element of $B$.
7. For finite sets $A$ and $B$, determine the lower and upper bounds of the cardinality of $A + B$. For infinite sets $A$ and $B$, determine the lower and upper asymptotic density of $A + B$.
8. For a finite set $A$, describe the cardinality and the structure of the $h$-fold sumset $hA$ as $h \to \infty$. For an infinite set $A$, describe the structure and an appropriate density of $hA$ as $h \to \infty$.

Finally, let us mention one of the many interesting open problems in additive number theory as follows.

9. (Erdös-Turan conjecture) For each $A \subseteq \mathbb{N}_0$ and $h \in \mathbb{N}$ let $r_{A,h}(n)$ be the number of (unordered) representations of $n$ as a sum of $h$ elements of $A$, that is, $r_{A,h}(n)$ is the cardinality of the set of all $h$-tuples $(a_1, a_2, \dots, a_h) \in A^h$ such that

   $$a_1 \le a_2 \le \cdots \le a_h \text{ and } a_1 + a_2 + \cdots + a_h = n.$$

   Erdös and Turan conjecture that if $A \subseteq \mathbb{N}_0$ is an asymptotic basis of order $h$, then

   $$\limsup_{n\to\infty} r_{A,h}(n) = \infty.$$

   This problem is still unsolved even for $h = 2$.

For more problems, we recommend the reader to search for them on the internet or attend the conference Combinatorial and Additive Number Theory (CANT) organized almost every year.

## 10.5. Schnirelmann's Basis Theorem

Goldbach's conjecture states that every even integer larger than 2 is a sum of two prime numbers. Schnirelmann was the first to give significant progress toward the solution to Goldbach's conjecture. Following Nathanson [**283**, pp. 193–199], we present the proof of Schnirelmann's basis theorem and use it to prove that every large even integer is a sum of a uniformly bounded number of primes.

We recall that for each $x > 0$ and a nonempty subset $A$ of $\mathbb{N}_0$, we write $A(x)$ to denote the number of elements in $A \cap [1, x]$. For each such $A$, define the Schnirelmann density $\sigma(A)$ by

$$\sigma(A) = \inf_{n \in \mathbb{N}} \frac{A(n)}{n}.$$

Then it is not difficult to see that $0 \le \sigma(A) \le 1$; $\sigma(A) = 1$ if and only if $A$ contains all positive integers; and if $1 \notin A$, then $\sigma(A) = 0$. We next give the following two lemmas, and then prove Schnirelmann's theorem.

**Lemma 10.21.** *Let $A, B \subseteq \mathbb{Z}$, $0 \in A \cap B$, and $n \in \mathbb{N}_0$.*

$$\text{If } A(n) + B(n) \ge n, \text{ then } n \in A + B.$$

**Proof.** If $0 \le n \le 2$, then the result can be easily checked. If $n \in A$, then $n = n + 0 \in A + B$. If $n \in B$, then $n = 0 + n \in A + B$. So assume that $n \notin A \cup B$, $n \ge 3$, and $A(n) + B(n) \ge n$. We first observe that the pairs of positive integers that have the sum equal to $n$ are $(1, n-1), (2, n-2), (3, n-3), \ldots, (n-1, 1)$. So we are looking for a pair $(x, y)$ from this list such that $x \in A$ and $y \in B$. This leads to the consideration of the following sets:

$$A_1 = \{n - a \mid a \in A \text{ and } 1 \le a \le n - 1\} \text{ and } B_1 = B \cap [1, n-1].$$

Then $A_1 \cup B_1 \subseteq [1, n-1]$, $|A_1| = A(n-1)$, and $|B_1| = B(n-1)$. Since $n \notin A \cup B$, we have $A(n-1) = A(n)$ and $B(n-1) = B(n)$. So

$$\begin{aligned} n - 1 + |A_1 \cap B_1| &\ge |A_1 \cup B_1| + |A_1 \cap B_1| = |A_1| + |B_1| \\ &= A(n) + B(n) \ge n. \end{aligned}$$

Therefore $|A_1 \cap B_1| \ge 1$. Hence there exists $a \in A$, $1 \le a \le n - 1$ such that $n - a \in B_1 \subseteq B$, and thus $n \in A + B$, as required. ☐

**Lemma 10.22.** *Let $A, B \subseteq \mathbb{Z}$ and $0 \in A \cap B$. If $\sigma(A) + \sigma(B) \ge 1$, then $n \in A + B$ for every $n \in \mathbb{N}_0$.*

**Proof.** By the definition of $\sigma(A)$ and $\sigma(B)$, for each $n \in \mathbb{N}$, we have

$$\frac{A(n)}{n} + \frac{B(n)}{n} \geq \sigma(A) + \sigma(B) \geq 1,$$

and so $n \in A + B$ by Lemma 10.21. □

**Theorem 10.23.** (Schnirelmann) *Let $A, B \subseteq \mathbb{Z}$ and $0 \in A \cap B$. Then*

$$\sigma(A + B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

**Proof.** It is enough to show that

$$\sigma(A) + \sigma(B) - \sigma(A)\sigma(B) \leq \frac{(A + B)(n)}{n} \quad \text{for all } n \in \mathbb{N}. \tag{10.21}$$

We would like to count as many of the integers in $(A + B) \cap [1, n]$ as possible, so that (10.21) holds. Let $a_0 = 0$ and let

$$1 \leq a_1 < a_2 < a_3 < \cdots < a_k \leq n$$

be the elements of $A$ in $[1, n]$. Since $0 \in B$, $a_i = a_i + 0 \in A + B$ for all $i$. Next, we are going to count the elements in $A + B$ that lie in each interval $(a_0, a_1), (a_1, a_2), \ldots, (a_{k-1}, a_k)$ and $(a_k, n]$. Let

$$1 \leq b_1 < b_2 < b_3 < \cdots < b_r \leq n$$

be the elements of $B \cap [1, n]$, and let $b_1, b_2, \ldots, b_{r_0}$ be all the elements of $B$ such that

$$a_0 < a_0 + b_1 < a_0 + b_2 < \cdots < a_0 + b_{r_0} < a_1.$$

Therefore $r_0 = B(a_1 - a_0 - 1)$. Next, let $b_1, b_2, b_3, \ldots, b_{r_1}$ be all the elements in $B$ such that

$$a_1 < a_1 + b_1 < a_1 + b_2 < \cdots < a_1 + b_{r_1} < a_2,$$

and so $r_1 = B(a_2 - a_1 - 1)$. In general, for each $i = 0, 1, 2, \ldots, k - 1$, let $b_1, b_2, \ldots, b_{r_i}$ be all the elements of $B$ such that

$$a_i < a_i + b_1 < a_i + b_2 < \cdots < a_i + b_{r_i} < a_{i+1},$$

and $r_i = B(a_{i+1} - a_i - 1)$. Finally, we count the integers in the set $(A + B) \cap (a_k, n]$. Let $b_1, b_2, \ldots, b_{r_k}$ be all the elements of $B$ such that

$$a_k < a_k + b_1 < a_k + b_2 < \cdots < a_k + b_{r_k} \leq n,$$

and so $r_k = B(n - a_k)$. Combining the count of the elements of $A + B$ from each step, we obtain

$$\begin{aligned}
(A+B)(n) &\geq k + \sum_{i=0}^{k} r_i \\
&= A(n) + \left( \sum_{i=0}^{k-1} B\left(a_{i+1} - a_i - 1\right) \right) + B\left(n - a_k\right) \\
&\geq A(n) + \sigma(B) \sum_{i=0}^{k-1} \left(a_{i+1} - a_i - 1\right) + \sigma(B)\left(n - a_k\right) \\
&= A(n) + \sigma(B) \sum_{i=0}^{k-1} \left(a_{i+1} - a_i\right) - \sigma(B)k + \sigma(B)\left(n - a_k\right) \\
&= A(n) + \sigma(B)n - \sigma(B)k \\
&= A(n) + \sigma(B)n - \sigma(B)A(n) \\
&= A(n)(1 - \sigma(B)) + \sigma(B)n \\
&\geq n\sigma(A)(1 - \sigma(B)) + n\sigma(B) \\
&= n\left(\sigma(A) + \sigma(B) - \sigma(A)\sigma(B)\right).
\end{aligned}$$

Therefore (10.21) holds and the proof is complete. □

There is a slightly different and stronger version of Theorem 10.23 as follows.

**Theorem 10.24.** (Schnirelmann Theorem Version 2) *Let* $A, B \subseteq \mathbb{Z}$, $0 \in A$, *and* $1 \in B$. *Then* $\sigma(A+B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B)$.

**Proof.** The proof is similar to that of Theorem 10.23, but we start with the elements of $B$ and insert the elements in $A+B$ between each interval. So let $n \in \mathbb{N}$ and $1 = b_1 < b_2 < b_3 < \cdots < b_r \leq n$ be the elements in $B \cap [1, n]$ and so $r = B(n)$. Since $0 \in A$, the $b_i$ are in $A + B$. Let $a_0 = 0$, and $1 \leq a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_k \leq n$ be the elements of $A \cap [1, n]$. For each $i = 1, 2, \ldots, r-1$, let $a_1 < a_2 < \cdots < a_{r_i}$ be all the elements in $a \in A$ such that $b_i < a + b_i \leq b_{i+1} - 1$, and so the number of such $a$ is $A(b_{i+1} - b_i - 1)$. For $i = r$, there are $A(n - b_k)$ elements $a \in A$ such that

$b_k < a + b_k \le n$. Collecting the count, we have

$$\begin{aligned}(A+B)(n) &\ge B(n) + \sum_{i=1}^{r-1} A(b_{i+1} - b_i - 1) + A(n - b_r)\\ &\ge r + \sigma(A)\sum_{i=1}^{r-1}(b_{i+1} - b_i - 1) + \sigma(A)(n - b_r)\\ &= r + \sigma(A)(b_r - b_1 - (r-1) + n - b_r)\\ &= r + \sigma(A)(n - r)\\ &= r(1 - \sigma(A)) + n\sigma(A)\\ &\ge (1 - \sigma(A))\sigma(B)n + n\sigma(A)\\ &= n(\sigma(A) + \sigma(B) - \sigma(A)\sigma(B)).\end{aligned}$$

This implies the desired result. □

It is not difficult to see that we can apply Theorem 10.24 to prove Theorem 10.23 since if $0 \in A \cap B$ and $1 \notin B$, then we obtain $\sigma(B) = 0$ and $A \subseteq A + B$. Nevertheless, Theorems 10.23 and 10.24 are not sharp. In fact, an optimal result was obtained by Mann [**258**], but the proof is more complicated and we do not need it here. Therefore we only state Mann's theorem as follows.

**Theorem 10.25.** (Mann's Theorem [**258**]) *Suppose* $A, B \subseteq \mathbb{Z}$ *and* $0$ *are in* $A \cap B$. *Then*

$$\sigma(A+B) \ge \min\{1, \sigma(A) + \sigma(B)\}.$$

**Example 10.26.** Let $m \ge 3$ be a positive integer and

$$A = B = \{0\} \cup \{n \in \mathbb{N} \mid n \equiv 1 \pmod{m}\}.$$

Then $\sigma(A) = \sigma(B) = \frac{1}{m}$, $A + B = \{0\} \cup \{n \in \mathbb{N} \mid n \equiv 1, 2 \pmod{m}\}$, and $\sigma(A+B) = \frac{2}{m}$. So $\sigma(A+B) = \sigma(A) + \sigma(B) < 1$. This shows that the inequality in Mann's theorem is sharp.

We emphasize that it is very important that $0 \in A \cap B$ or ($0 \in A$ and $1 \in B$) in order to apply Schnirelmann's or Mann's theorem as the following example shows.

**Example 10.27.** (The importance of zero and one in the sumset) Suppose $A = \mathbb{N}_0$ and $B = \{2\}$. Then $0 \notin B$, $1 \notin B$, $\sigma(A) = 1$, $\sigma(B) = 0$,

$A+B=\mathbb{Z}\cap[2,\infty)$, and $\sigma(A+B)=0$, and so

$$\begin{aligned}\sigma(A)+\sigma(B)-\sigma(A)\sigma(B)&=1>\sigma(A+B)\\ \min\{1,\sigma(A)+\sigma(B)\}&=1>\sigma(A+B).\end{aligned}$$

This shows that the assumption $0\in A\cap B$ in Schnirelmann's and Mann's theorem cannot be omitted.

**Example 10.28.** (The importance of 1 in the sumset) Suppose $A$ and $B$ are subsets of $\mathbb{Z}$ and $0\in A\cap B$. If $1\notin A$ and $1\notin B$, and we apply Schnirelmann's or Mann's theorem, then the information we obtain is that $\sigma(A+B)\geq 0$, which is trivial. Furthermore, if $1\in A$ but $1\notin B$, then these theorems only tell us that $\sigma(A+B)\geq\sigma(A)$, which is trivial because we also know that $0\in B$ and so $A\subseteq A+B$. Similarly, if $1\in B$ but $1\notin A$, then we do not get anything new from applying these theorems. Hence, in order to apply Schnirelmann's and Mann's theorem effectively, it is important to have $1\in A\cap B$.

There is a slightly different version of Lemma 10.22 too. We give it as an exercise as follows.

**Exercise 10.29.** Let $A,B\subseteq\mathbb{Z}$, $0\in A$, $1\in B$, and $\sigma(A)+\sigma(B)\geq 1$. This exercise is an outline of the proof that $A+B$ contains every positive integer.

(i) Suppose that $\mathbb{N}\not\subseteq A+B$. Let $n$ be the smallest positive integer that is not in $A+B$. Show that $n\geq 2$ and $n\notin B$.

(ii) Let

$$\begin{aligned}A_1&=\{a\mid a\in A\text{ and }1\leq a\leq n-1\},\\ B_1&=\{n-b\mid b\in B\text{ and }1\leq b\leq n-1\}.\end{aligned}$$

Show that $A_1\cap B_1=\emptyset$, $|A_1|=A(n-1)$, $|B_1|=B(n-1)$, and $|A_1|+|B_1|\leq n-1$.

(iii) Show that $A(n-1)+B(n-1)>(\sigma(A)+\sigma(B))(n-1)\geq n-1$.

(iv) Conclude that $\mathbb{N}\subseteq A+B$.

Theorem 10.23 can also be written as

$$1-\sigma(A+B)\leq(1-\sigma(A))(1-\sigma(B))$$

which can be generalized to $h$ sets of integers as follows:

**Theorem 10.30.** *Let $A_1, A_2, \dots, A_h$ be sets of integers and $0 \in A_i$ for all $i = 1, 2, \dots, h$. Then*

$$1 - \sigma(A_1 + A_2 + \cdots + A_h) \le \prod_{i=1}^{h} (1 - \sigma(A_i)).$$

**Proof.** The idea is to group each term and use Theorem 10.23 repeatedly as follows:

$$\begin{aligned}
1-&\sigma(A_1 + (A_2 + \cdots + A_h)) \\
&\le (1 - \sigma(A_1))(1 - \sigma(A_2 + \cdots + A_h)) \\
&\le (1 - \sigma(A_1))(1 - \sigma(A_2))(1 - \sigma(A_3 + \cdots + A_h)) \\
&\ \ \vdots \\
&\le \prod_{i=1}^{h} (1 - \sigma(A_i)).
\end{aligned}$$

This completes the proof. □

**Theorem 10.31.** (Schnirelmann Basis Theorem) *If $A \subseteq \mathbb{Z}$, $0 \in A$, and $\sigma(A) > 0$, then $A$ is a basis of finite order.*

**Proof.** Let $\sigma(A) = x$. Then $0 \le 1 - x < 1$. Then

$$1 - \sigma(hA) \le (1 - x)^h \le \frac{1}{2},$$

for some large $h \in \mathbb{N}$. Then $\sigma(hA) \ge \frac{1}{2}$ and so $\sigma(hA) + \sigma(hA) \ge 1$. By Lemma 10.22, $n \in hA + hA = 2hA$ for every $n \in \mathbb{N}$. This completes the proof. □

Next, we will apply Schnirelmann's basis theorem to show that every integer larger than 1 is a sum of a uniformly bounded number of primes. We first need to show that the set $A$ consisting of 0, 1, and $p + q$ where $p$, $q$ ranges over all primes has positive Schnirelmann density. To do this, we need an estimate for the average of the number of (ordered) representations of $N$ as a sum of two primes. Here ordered representation means that each different order of the summands is counted as a distinct representation.

**Lemma 10.32.** *Let $r(N)$ be the number of ordered representations of $N$ as a sum of two primes. Then we have*

$$\sum_{N\le x} r(N) \gg \frac{x^2}{(\log x)^2} \text{ and } \sum_{N\le x} (r(N))^2 \ll \frac{x^3}{(\log x)^4}.$$

**Proof.** If $p_1 < p_2 < \cdots < p_k$ are the primes at most $x/2$, then $p_i+p_j \le x$ for all $i, j \le k$, and so $p_i + p_j$ is counted as one of the representations of integers at most $x$. Therefore

$$\sum_{N\le x} r(N) \ge (\pi(x/2))^2 \gg \left(\frac{x/2}{\log(x/2)}\right)^2 \gg \frac{x^2}{(\log x)^2}.$$

Next, we recall from Theorem 10.10 that for an even positive integer $N$, we have

$$r(N) \ll \frac{N}{(\log N)^2} \prod_{p|N}\left(1+\frac{1}{p}\right) \le \frac{N}{(\log N)^2}\sum_{d|N}\frac{1}{d}.$$

If $N$ is odd and $N$ is a sum of two primes, then one of the primes must be 2 and the other is $N-2$, and so $N = 2+(N-2) = (N-2)+2$ are the only possible representations of $N$ as a sum of two primes. Therefore

$$r(N) \le 2 \le \frac{N}{(\log N)^2}\sum_{d|N}\frac{1}{d} \quad \text{for every odd integer } N \ge 3,$$

where the last inequality follows from the fact that $x \ge 2(\log x)^2$ for all $x \ge 9$. Therefore

$$\begin{aligned}
\sum_{N\le x}(r(N))^2 &\ll \sum_{N\le x}\frac{N^2}{(\log N)^4}\left(\sum_{d|N}\frac{1}{d}\right)^2 \\
&\ll \frac{x^2}{(\log x)^4}\sum_{N\le x}\sum_{d_1|N}\sum_{d_2|N}\frac{1}{d_1d_2} \\
&= \frac{x^2}{(\log x)^4}\sum_{d_1,d_2\le x}\frac{1}{d_1d_2}\sum_{\substack{N\le x\\ d_1|N,\, d_2|N}} 1 \\
&\ll \frac{x^2}{(\log x)^4}\sum_{d_1,d_2\le x}\frac{1}{d_1d_2}\frac{x}{[d_1,d_2]}. \qquad (10.22)
\end{aligned}$$

By considering the exponents in prime factorizations and observing that $\max\{a, b\} \geq (a+b)/2$ for any $a, b \geq 0$, we see that

$$[d_1, d_2] \geq (d_1 d_2)^{\frac{1}{2}}.$$

So (10.22) implies that

$$\begin{aligned}\sum_{N \leq x} (r(N))^2 &\ll \frac{x^3}{(\log x)^4} \sum_{d_1, d_2 \leq x} \frac{1}{d_1^{\frac{3}{2}} d_2^{\frac{3}{2}}} \\ &= \frac{x^3}{(\log x)^4} \left( \sum_{d \leq x} \frac{1}{d^{\frac{3}{2}}} \right)^2 \ll \frac{x^3}{(\log x)^4}.\end{aligned}$$

This completes the proof. ☐

**Theorem 10.33.** *Let* $A = \{0, 1\} \cup \{p + q \mid \ p$ *and* $q$ *are primes*$\}$. *Then* $\sigma(A) > 0$.

**Proof.** By Cauchy's inequality, we have

$$\left( \sum_{N \leq x} r(N) \right)^2 \leq \left( \sum_{\substack{N \leq x \\ r(N) \geq 1}} 1 \right) \left( \sum_{N \leq x} (r(N))^2 \right) \leq A(x) \sum_{N \leq x} (r(N))^2.$$

By Lemma 10.32, we obtain

$$\frac{A(x)}{x} \geq \frac{1}{x} \frac{\left( \sum_{N \leq x} r(N) \right)^2}{\sum_{N \leq x} (r(N))^2} \gg \frac{1}{x} \frac{x^4/(\log x)^4}{x^3/(\log x)^4} \gg 1.$$

This implies that there exists $c > 0$ such that $A(x) \geq cx$ for all $x \geq x_0$. In addition, $A(1) > 0$, and so $A(x) > 0$ for all $1 \leq x \leq x_0$. Therefore

$$\sigma(A) \geq \min\left\{ \frac{A(1)}{1}, \frac{A(2)}{2}, \ldots, \frac{A(\lfloor x_0 \rfloor)}{\lfloor x_0 \rfloor}, c \right\} > 0.$$

This completes the proof. ☐

**Theorem 10.34.** (Schnirelmann's Theorem) *Every integer greater than one is a sum of a uniformly bounded number of primes. In other words, there exists* $N \in \mathbb{N}$ *such that every integer larger than one can be written as a sum of at most* $N$ *prime numbers.*

**Proof.** Let $A$ be the set defined in Theorem 10.33. By the Schnirelmann basis theorem, there exists $h \in \mathbb{N}$ such that $hA$ contains all nonnegative integers. To prove the theorem, let $n \geq 2$ be a positive integer. We show that $n$ can be written as a sum of at most $1 + 2h$ primes. If $n \leq 5$, then the result is easy to check. So let $n \geq 6$. Since $n - 2 \in hA$, there exist integers $k, \ell$ such that

$$n - 2 = 1 + 1 + \cdots + 1 + (p_1 + q_1) + (p_2 + q_2) + \cdots + (p_\ell + q_\ell) \tag{10.23}$$

where $k, \ell \geq 0$, the $p_i$, $q_i$ are primes, the number of 1's in (10.23) is $k$, and $k + \ell \leq h$. If $k$ is even, we can write (10.23) as

$$n = 2 + 2 + \cdots + 2 + (p_1 + q_1) + (p_2 + q_2) + \cdots + (p_\ell + q_\ell),$$

where there are $1 + k/2 + 2\ell$ primes in the above sum. If $k$ is odd, then we write (10.23) as

$$n = 3 + 2 + 2 + \cdots + 2 + (p_1 + q_1) + (p_2 + q_2) + \cdots + (p_\ell + q_\ell),$$

where there are $1 + \frac{k-1}{2} + 2\ell$ primes in the above sum. In any case, $n$ is a sum of at most $N$ primes, where

$$N = 1 + \frac{k}{2} + 2\ell \leq 1 + \frac{h - \ell}{2} + 2\ell = 1 + \frac{h + 3\ell}{2} \leq 1 + 2h.$$

This completes the proof. □

We end this section by giving one of Nathanson's favorite problems presented at the conference CANT2020, which should be compared with the Schnirelmann basis theorem.

**Problem 10.35.** Let $A \subseteq \mathbb{N}_0$ and let the lower asymptotic density of $A$ satisfy $\underline{D}(hA) = 0$ for all $h \in \mathbb{N}$. Describe the structure of $A$ and the evolution of the structures of $hA$ as $h \to \infty$.

## 10.6. An Outline of the Circle Method in Waring's Problem

Continuing from Examples 10.15 and 10.16, we give an outline of the solution to Waring's problem by using the circle method. We follow closely the complete proof given in the book by Davenport [**99**]. The book by Vaughan [**422**] is a classic reference for anyone who is interested in the circle method while the one by Davenport [**99**] covers less but is easier to read. So we use Davenport [**99**] as the main reference in our presentation.

Waring's problem is to show that for each integer $k \geq 2$, there exists $s = s_k \in \mathbb{N}$ such that every positive integer $N$ can be written as

$$N = x_1^k + x_2^k + \cdots + x_s^k \tag{10.24}$$

where $x_i$ is a nonnegative integer for all $i$. The existence of such $s = s_k$ is not obvious, and even after the existence of such an $s$ is established, the calculation of the smallest such $s$ is still difficult. Nevertheless, suppose for now that we only are interested in proving the existence of such an $s$. Then it is in fact enough to show that (10.24) holds for every sufficiently large integer $N \geq N_0$ since we can always write the integer $n \in [1, N_0]$ as $n = 1^k + 1^k + \cdots + 1^k + 0^k + 0^k + \cdots + 0^k$, where the number of $1^k$ and $0^k$ are $n$ and $N_1 - n$, respectively, where $N_1 = \max\{N_0, s_k\}$. Therefore the classical Waring's problem is solved if and only if the modern version is solved (see also a more general situation in Example 10.20). Thus we can always assume that $N$ is large. Nevertheless, we emphasize from Example 10.17 that the determination of $G(k)$ in the modern Waring's problem is much more difficult than that of $g(k)$ in the classical one.

Recall that $e(t) = e^{2\pi i t}$ for each $t \in \mathbb{R}$. Define $T(\alpha)$ for each $\alpha \in \mathbb{R}$ by,

$$T(\alpha) = \sum_{x=1}^{P} e\left(\alpha x^k\right),$$

where $P$ is a positive integer. Then

$$(T(\alpha))^s = \sum_m r(m) e(\alpha m) \tag{10.25}$$

where $r(m)$ is the number of representations of $m$ as in (10.24) with $1 \leq x_i \leq P$ for all $i = 1, 2, \ldots, s$. Multiplying both sides of (10.25) by $e(-N\alpha)$ and integrate over $\alpha$ in the interval $[0, 1]$, we obtain

$$r(N) = \int_0^1 (T(\alpha))^s e(-N\alpha)\, d\alpha. \tag{10.26}$$

Then Waring's problem is solved if we can show that $r(N) > 0$ for all sufficiently large $N$. In fact, we can obtain an asymptotic formula for $r(N)$ as follows.

**Theorem 10.36.** *Let $k \geq 2$, $s \geq 2^k + 1$, $r(N)$ be the number of representations of $N$ as in* (10.24) *with $x_i \geq 1$ for all $i$. Then*

$$r(N) = C_{k,s} N^{\frac{s}{k}-1} \mathfrak{S}(N) + O\left(N^{\frac{s}{k}-1-\delta}\right), \tag{10.27}$$

*where* $\delta > 0$ *is fixed,* $\mathfrak{S}(N) \geq \gamma > 0$ *for some constant* $\gamma$ *independent of* $N$*, and*

$$C_{k,s} = \frac{\Gamma\left(1+\frac{1}{k}\right)^s}{\Gamma\left(\frac{s}{k}\right)} > 0.$$

In the above formula, $\mathfrak{S}(N)$ is an infinite series, which Hardy and Littlewood called the singular series. By (10.27), we see that

$$r(N) \sim C_{k,s} N^{\frac{s}{k}-1} \mathfrak{S}(N) \text{ as } N \to \infty,$$

and therefore $r(N) > 0$ for all sufficiently large $N$, as required. The important tools for the proof of Theorem 10.36 are Weyl's and Hua's inequalities as follows.

**Lemma 10.37.** (Weyl's Inequality) *Let* $f(x)$ *be a real polynomial of degree* $k$ *with highest coefficient* $\alpha$*:*

$$f(x) = \alpha x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k.$$

*Suppose that* $\alpha$ *has a rational approximation* $a/q$ *satisfying*

$$(a, q) = 1, \quad q > 0, \quad \left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}.$$

*Then, for any* $\varepsilon > 0$*,*

$$\left|\sum_{x=1}^{P} e(f(x))\right| \ll P^{1+\varepsilon}\left(P^{-1} + q^{-1} + qP^{-k}\right)^{\frac{1}{K}},$$

*where* $K = 2^{k-1}$ *and the implied constant depends only on* $k$ *and* $\varepsilon$*.*

**Lemma 10.38.** (Hua's Inequality) *If*

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k),$$

*then*

$$\int_0^1 |T(\alpha)|^{2^k} d\alpha \ll P^{2^k - k - \varepsilon}$$

*for any fixed* $\varepsilon > 0$*.*

The proof of Lemmas 10.37 and 10.38 can be found, for example, in [**99**, pp. 8-13] and [**422**, pp. 11-13].

After obtaining these lemmas, we now return to the proof of Theorem 10.37.

Let $P = \left\lfloor N^{\frac{1}{k}} \right\rfloor$ and recall that $T(\alpha) = \sum_{1 \le x \le P} e(\alpha x^k)$,

and

$$r(N) = \int_0^1 (T(\alpha))^s e(-N\alpha) d\alpha. \tag{10.28}$$

Since we expect the main term of $r(N)$ to be of order $N^{\frac{s}{k}-1}$ or $P^{s-k}$, so we can disregard any set values of $\alpha$ in (10.28) that contribute to the integral an amount which is of strictly smaller order than $P^{s-k}$. We suppose $s \ge 2^k + 1$, and if we write the absolute value of the integrand as $|T(\alpha)|^{s-2^k} |T(\alpha)|^{2^k}$ and apply Hua's inequality, we see that we can disregard any set of $\alpha$ for which $|T(\alpha)| \ll P^{1-\delta}$ for some fixed $\delta > 0$. So we divide the set of $\alpha \in [0, 1]$ into two sets called the major arcs and the minor arcs, respectively. The set of $\alpha$ in major arcs contributes to the main term while the set of $\alpha$ in minor arcs goes to the error term. The major arcs are defined for $1 \le q \le P^{\delta}$, $1 \le a \le q$, $(a, q) = 1$, by

$$\mathfrak{M}(a, q) = \left\{ \alpha \in \mathbb{R} \ : \ \left| \alpha - \frac{a}{q} \right| < P^{-k+\delta} \right\}.$$

The minor arcs $\mathfrak{m}$ are defined by $\mathfrak{m} = [0, 1] \setminus \bigcup \mathfrak{M}(a, q)$, where the union is taken over all $1 \le q \le P^{\delta}$, $1 \le a \le q$, $(a, q) = 1$. Then the contributions to the integral from each $\alpha$ are obtained from the following lemma.

**Lemma 10.39.** *If $s \ge 2^k + 1$, we have*

$$\int_{\mathfrak{m}} |T(\alpha)|^s \, d\alpha \ll P^{s-k-\delta'}$$

*where $\delta'$ is a positive number depending on $\delta$.*

**Lemma 10.40.** *For $\alpha$ in $\mathfrak{M}(a, q)$, putting $\alpha = \beta + a/q$, we have*

$$T(\alpha) = q^{-1} S_{a,q} I(\beta) + O\left(P^{2\delta}\right),$$

*where*

$$S_{a,q} = \sum_{z=1}^{q} e\left(az^k/q\right),$$

$$I(\beta) = \int_0^P e\left(\beta\zeta^k\right) d\zeta.$$

**Lemma 10.41.** *Let* $\mathfrak{M}$ *be the union of all major arcs* $\mathfrak{M}(a,q)$. *Then*

$$\int_{\mathfrak{M}} (T(\alpha))^s e(-N\alpha)d\alpha = P^{s-k}\mathfrak{S}(P^\delta, N)J(P^\delta) + O\left(P^{s-k-\delta'}\right)$$

*for some* $\delta' > 0$, *where*

$$\mathfrak{S}(P^\delta, N) = \sum_{q \le P^\delta} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(q^{-1}S_{a,q}\right)^s e\left(-Na/q\right),$$

$$J(P^\delta) = \int_{|\gamma|<P^\delta} \left(\int_0^1 e\left(\gamma\zeta^k\right) d\zeta\right)^s e(-\gamma)d\gamma.$$

The proof of Lemmas 10.39 to 10.41 can be found in [**99**, pp. 16-20] and [**422**, pp. 14-17].

By (10.28) and Lemmas 10.39 and 10.41, we write $r(N)$ as the integral on $\mathfrak{M}$ and $\mathfrak{m}$ to obtain

$$r(N) = P^{s-k}\mathfrak{S}(P^\delta, N)J(P^\delta) + O\left(P^{s-k-\delta'}\right). \tag{10.29}$$

After this point, there is still a long calculation. The idea is to replace $J(P^\delta)$ by $J$ and $\mathfrak{S}(P^\delta, N)$ by $\mathfrak{S}(N)$ with errors which are permissible. Then we have to show that $J = C_{k,s}$. The complete proof can be found in Davenport [**99**, pp. 20–21].

We do not really give any detail here because it is beyond the scope of this book. If the reader would like to read more about the circle method, we again recommend the books by Davenport [**99**] and Vaughan [**422**], and the survey article by Vaughan and Wooley [**426**].

## Chapter 11

# Hints for Selected Exercises

### Hints for Exercises 1.13

1.13.1 Show that

$$[a,b,c](ab,ac,bc) = abc, [a,b,c,d](abc,abd,acd,bcd) = abcd,$$

and in general,

$$[a_1,a_2,\dots,a_n]M = a_1a_2\cdots a_n,$$

where $M$ is the greatest common divisors of the numbers that are products of any $n-1$ distinct numbers chosen from $a_1,a_2,\dots,a_n$.

**Hint.** Calculate the $p$-adic valuations of each side. If $m$ and $n$ are positive integers and $v_p(m) = v_p(n)$ for all $p$, then $m = n$.

1.13.3 Prove that every $n \geq 12$ is the sum of two composite numbers.

**Hint.** $n = n-4+4 = n-9+9$.

1.13.5 Prove that if $2^n+1$ is prime, then $n$ is a power of 2.

**Hint.** If $n$ is odd, then

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \cdots + y^{n-1}).$$

1.13.7 Let $a,b \in \mathbb{N}$ and $(a,b) = 1$. Prove the following statements.

(i) There exist positive integers $x$ and $y$ such that $ax - by = 1$.

(ii) For every $n > ab$ there exist positive integers $x$ and $y$ such that $n = ax + by$.

(iii) There are no positive integers $x$ and $y$ such that $ab = ax + by$.

**Hint.** For (ii), use (i) and Theorem 1.8. Alternatively, show that the set of $n - a, n - 2a, \dots, n - ba$ forms a complete residue system modulo $b$.

1.13.9 Show that there are infinitely many $n \in \mathbb{N}$ such that $n$, $n + 1$, $n+2$ are sums of two squares. Show also that any set of four consecutive integers contains an element that is not a sum of two squares. Hint: if $n$, $n+1$, $n+2$ are sum of two squares, so is $n(n+2)$, $n^2+2n+1$, $n^2+2n+2$.

**Hint.** If $n$, $n+1$, $n+2$ are sum of two squares, so are $n(n+2)$, $n^2+2n+1$, $n^2 + 2n + 2$.

## Hints for Exercises 2.6

2.6.3 Let $\gamma(1) = 1$ and $\gamma(n) = \prod_{p|n} p$ for each $n > 1$. Show that

$$\sum_{k|n} d(k) = \frac{d(n)d(n\gamma(n))}{2^{\omega(n)}}.$$

**Hint.** Use Theorem 2.22.

2.6.5 If $f = \mu * \omega$, prove that for each $n \in \mathbb{N}$, $f(n)$ is either 0 or 1. Similarly, show that if $f = \mu * \Omega$, then $f(n) \in \{0, 1\}$ for all $n \in \mathbb{N}$.

**Hint.** As in the proof of Theorem 2.17, we can calculate directly and use the binomial theorem. Alternatively, let $g(n)$ be equal to 1 if $n$ is prime and 0 otherwise, consider $\sum_{d|n} g(d)$, and use the Möbius inversion formula.

2.6.10 Prove that $\varphi(n) > n/6$ for all $n$ with at most eight distinct prime factors.

**Hint.** $\varphi(n)/n = \prod_{p|n}(1 - 1/p)$ and $1 - 1/p$ is small when $p$ is small.

2.6.12 Prove that $\prod_{t|n} t = n^{d(n)/2}$.

**Hint.** If $u \mid n$, then there exists $v \mid n$ such that $uv = n$. You may need to separate the case when $n$ is a square where $d(n)$ is odd and $\sqrt{n}$ is a divisor of $n$.

2.6.15 Let $\tau(n)$ be the number of positive divisors of $n$. Prove that the following equalities hold for all $n \in \mathbb{N}$.

(i) $\displaystyle\sum_{d|n} \sigma(d) = n \sum_{d|n} \frac{\tau(d)}{d}$.

(ii) $\displaystyle\sum_{d|n} \varphi(d)\tau\left(\frac{n}{d}\right) = \sigma(n)$.

(iii) $\displaystyle\sum_{d|n} \varphi(d)\sigma\left(\frac{n}{d}\right) = n\tau(n)$.

(iv) $\displaystyle\sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\tau(d)$.

(v) $\displaystyle\sum_{d|n} d\sigma(d) = \sum_{d|n} \left(\frac{n}{d}\right)^2 \sigma(d)$

(vi) $\displaystyle\sum_{d|n} \sigma(d)\sigma\left(\frac{n}{d}\right) = \sum_{d|n} d\tau(d)\tau\left(\frac{n}{d}\right)$.

**Hint.** Every function in the problem is multiplicative.

2.6.16 Let $P(n)$ be as in Example 2.36. Compute $P(n)$ without using Theorem 2.35.

**Hint.** $P(n) = \prod_{\ell \le n} \ell^{\sum_{d|(\ell,n)} \mu(d)} = \prod_{\ell \le n} \prod_{d|(\ell,n)} \ell^{\mu(d)}$.

2.6.17 Let $f(x)$ be defined for all rational $x$ in $[0,1]$ and let

$$F(n) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right) \quad \text{and} \quad F_1(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} f\left(\frac{k}{n}\right).$$

(i) Show that $F_1 = \mu * F$.

(ii) Prove that $\mu(n)$ is the sum of the primitive $n$th roots of unity:

$$\mu(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} e^{2\pi i k/n}.$$

**Hint.** See Theorem 2.21.

## Hints for Exercises 3.5

3.5.5 Let $x \in \mathbb{R}$, $m \in \mathbb{Z}$, and $n \in \mathbb{N}$. Show that

(i) $\left\lfloor\frac{m+\lfloor -x\rfloor}{n}\right\rfloor = \left\lfloor\frac{m-x}{n}\right\rfloor$,

(ii) $\left\lceil\frac{m+\lceil -x\rceil}{n}\right\rceil = \left\lceil\frac{m-x}{n}\right\rceil$,

(iii) $\left\lceil\frac{m+\lfloor -x\rfloor}{n}\right\rceil = \left\lceil\frac{m-x-[x\notin\mathbb{Z}]}{n}\right\rceil$,

(iv) $\left\lfloor\frac{m+\lceil -x\rceil}{n}\right\rfloor = \left\lfloor\frac{m-x+[x\in\mathbb{Z}]}{n}\right\rfloor$.

**Hint.** Apply Theorem 3.3(v) and Corollary 3.5.

3.5.10 Let $f(x) = x - \lfloor x\rfloor - \frac{1}{2}$ for every $x \in \mathbb{R}$. Show that

$$\left|\sum_{n=1}^{m} f\left(2^n x + \frac{1}{2}\right)\right| \le 1 \quad \text{for all } m \ge 1 \text{ and all } x \in \mathbb{R}.$$

**Hint.** Apply the result in Example 3.14. Write the sum as

$$\sum_{n=1}^{m} f\left(2^n\left(x + \frac{1}{2^{n+1}}\right)\right).$$

3.5.12 Let $m, n \in \mathbb{N}$ be odd and $\gcd(m,n) = 1$. Let $a = (n-1)/2$, $b = (m-1)/2$.

(i) Prove that $\sum_{r=1}^{a}\lfloor mr/n\rfloor + \sum_{r=1}^{b}\lfloor nr/m\rfloor = ab$.

(ii) Obtain a corresponding result if $(m,n) = d$.

**Hint.** If $(m,n) = d$ and $m_1 = \frac{m}{d}$, $n_1 = \frac{n}{d}$, then $(m_1, n_1) = 1$ and $m/n = m_1/n_1$. Alternatively, we can apply Theorem 3.18 to the function $f(x) = \frac{m}{n}x$ and follow the argument used in Example 3.27.

3.5.15 Prove that

$$\sum_{k=1}^{n}\left\lfloor\frac{k}{2}\right\rfloor = \left\lfloor\frac{n^2}{4}\right\rfloor$$

and that

$$\sum_{k=1}^{n}\left\lfloor\frac{k}{3}\right\rfloor = \left\lfloor\frac{n(n-1)}{6}\right\rfloor.$$

**Hint.** Consider the sum according to the size of $\left\lfloor\frac{k}{2}\right\rfloor$ as follows : $k = 0, 1$, $k = 2, 3$, $k = 4, 5, \dots$ which gives $\left\lfloor\frac{k}{2}\right\rfloor = 0, 1, 2, \dots$, respectively. If $n$ is odd, then $\sum_{k=1}^{n}\left\lfloor \frac{k}{2}\right\rfloor = \sum_{\ell=0}^{\frac{n-1}{2}}\sum_{k=2\ell}^{2\ell+1}\left\lfloor\frac{k}{2}\right\rfloor$. If $n$ is even, then the sum is $\sum_{\ell=0}^{\frac{n}{2}}\sum_{k=2\ell}^{2\ell+1}\left\lfloor\frac{k}{2}\right\rfloor - \left\lfloor\frac{n+1}{2}\right\rfloor$.

3.5.19 Let $p$ be a prime and $n \in \mathbb{N}$. Show that

$$\frac{n}{p-1} - \left\lfloor \frac{\log n}{\log p} \right\rfloor - 1 \le v_p(n!\,) \le \frac{n-1}{p-1}.$$

Prove also that $\frac{n}{p} - 1 < v_p(n!\,) < \frac{n}{p} + \frac{n}{p(p-1)}$.

**Hint.** If $n = (a_k a_{k-1} \cdots a_0)_p$, $a_k \ne 0$, then

$$s_p(n) \le (p-1)(k+1) = (p-1)\left(\left\lfloor \frac{\log n}{\log p} \right\rfloor + 1\right).$$

## Hints for Exercises 4.8

4.8.2 Show that for $x \ge 2$,

(i) $\sum_{n\le x} \log \frac{x}{n} = x + O(\log x)$,

(ii) $\sum_{n\le x} \left(\log \frac{x}{n}\right)^2 = 2x + O((\log x)^2)$.

In general, prove that $\displaystyle\sum_{n\le x} \left(\log \frac{x}{n}\right)^k = k!\,x + O((\log x)^k)$ for $k \ge 1$.

**Hint.** Write $\log \frac{x}{n} = \log x - \log n$. Use the binomial theorem. To prove a general result, use induction on $k$.

4.8.4 Let $x_1 = a$, $x_2 = b$, and $x_n = \frac{1}{2}(x_{n-1} + x_{n-2})$ for $n \ge 3$. Show that the series $\sum_{n=1}^{\infty} \frac{(-1)^n x_{2n}}{\log 2n}$ and $\sum_{n=1}^{\infty} \frac{(-1)^n x_{2n-1}}{\log 2n}$ are convergent.

**Hint.** Abel's test and alternating series test.

4.8.7 Show that $e$ is irrational.

**Hint.** Recall that $e = \sum_{m=0}^{\infty} \frac{1}{m!}$. If $e = a/b$, then consider

$$n!\,a - bn!\left(\sum_{m=0}^{n} \frac{1}{m!}\right).$$

If $n > b$, it is an integer and is also equal to $b\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots\right)$.

4.8.9 Prove that $e\left(\frac{n}{e}\right)^n < n! < en\left(\frac{n}{e}\right)^n$ for every $n \ge 2$.

**Hint.** Consider $\sum_{m \le n} \log m$ and apply Theorem 4.6.

4.8.12 Prove the following statements.

(i) $B_n(x+1) - B_n(x) = nx^{n-1}$ for $n \geq 1$,

(ii) $B_n(1) = B_n(0)$ for all $n \geq 2$,

(iii) $B_n = \sum_{k=0}^{n} \binom{n}{k} B_k$ for $n \geq 2$.

**Hint.** We have $\frac{ze^{(x+1)z}}{e^z - 1} - \frac{ze^{xz}}{e^z - 1} = ze^{xz}$.

4.8.17 Let $n \geq 2$. Prove the following statements.

(i) The function $x \mapsto B_n(\{x\})$ has period one.

(ii) The function $x \mapsto B_n(\{x\})$ is continuous on $\mathbb{R}$.

(iii) If $n \geq 3$, then the function $x \mapsto B_n(\{x\})$ is differentiable on $\mathbb{R}$.

**Hint.** We observe that $\{x+1\} = \{x\}$. First show that $B_n(\{x\})$ is continuous on $(0, 1)$. Then apply the result from Exercise 4.8.16.

## Hints for Exercises 5.6

5.6.8 Prove that for all $x \geq 1$, we have

(i) $\sum\limits_{n \le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1$, and

(ii) $\left| \sum\limits_{n \le x} \frac{\mu(n)}{n} \right| \leq 1$.

**Hint.** For (ii), start with (i) and write

$$\left| x \sum_{n \le x} \frac{\mu(n)}{n} \right| = \left| 1 + \sum_{n \le x} \mu(n) \left\{ \frac{x}{n} \right\} \right| = \left| 1 + \{x\} + \sum_{1 < n \le x} \mu(n) \left\{ \frac{x}{n} \right\} \right|.$$

5.6.13 In the proof of Theorem 5.23, we show that $\sigma(n)/n < n/\varphi(n)$ for $n \geq 2$. In Chapter 8, we will prove that the infinite product $\prod_p (1 - p^{-2})$, extended over all primes, converges to $6/\pi^2$. Assuming this result, prove that

(i) $\frac{\sigma(n)}{n} < \frac{n}{\varphi(n)} < \frac{\pi^2}{6} \frac{\sigma(n)}{n}$ for $n \geq 2$ and

(ii) $\sum_{n\leq x} \frac{n}{\varphi(n)} \asymp x.$

**Hint.** Apply Theorem 2.22 on $\sigma(n)/n$. Use the formula

$$\varphi(n) = n\prod_{p|n}(1 - 1/p)$$

and the relation $1 + x + x^2 + \cdots = \frac{1}{1-x} = \frac{1+x}{1-x^2}$ with $x = 1/p$.

5.6.15 Show that for $x \geq 2$,

$$\sum_{n\leq x} \frac{1}{\varphi(n)} \asymp \log x.$$

**Hint.** Use Exercise 5.6.13.

5.6.18 Suppose $f$ is an additive function. Show that

$$\sum_{n\leq x} f(n) = x\sum_{p\leq x}\frac{f(p)}{p} + x\sum_{\substack{p^a\leq x\\ a\geq 2}}\frac{f(p^a) - f(p^{a-1})}{p^a}$$

$$-\sum_{\substack{p^2\leq x\\ a\geq 1}}\left(f(p^a) - f(p^{a-1})\right)\left\{\frac{x}{p^2}\right\}.$$

Then use the above to prove that

(i) $\sum_{n\leq x}\omega(n) = x\log\log x + bx + O\left(\frac{x}{\log x}\right),$

(ii) $\sum_{n\leq x}\Omega(n) = x\log\log x + cx + O\left(\frac{x}{\log x}\right),$

where $b$ and $c$ are constants and $c - b = \sum_p \frac{1}{p(p-1)}$. You may use the fact that $\pi(x) \ll \frac{x}{\log x}$ for $x \geq 2$ and that $\sum_{p\leq x}\frac{1}{p} = \log\log x + b + O\left(\frac{1}{\log x}\right)$, which is proved in the next chapter.

**Hint.** Write $f(n) = \sum_{p^a\|n} f(p^a) = \sum_{\substack{p^a|n\\ a\geq 1}} f(p^a) - f(p^{a-1})$ and change the order of summation.

5.6.21 Prove the following statements.

(i) $d(n) \leq \sqrt{3n}$ for all $n \in \mathbb{N}$ and the equality occurs if and only if $n = 12$.

(ii) $d(n) \leq 8\sqrt[3]{3n/35}$ for all $n \in \mathbb{N}$ and the equality occurs if and only if $n = 2520$.

(iii) $d(n) \leq 96\sqrt[4]{3n/50050}$ for all $n \in \mathbb{N}$ and the equality occurs if and only if $n = 21621600$.

**Hint.** Modify the proof of Theorem 5.11. For each prime $p$ and $\varepsilon > 0$ such that $p^{\varepsilon} < 2$, let $f_p(x) = \frac{x+1}{p^{\varepsilon x}}$ for all $x \geq 0$. Then $f_p'(x) > 0$ if and only if $0 \leq x < \frac{1}{\varepsilon \log p} - 1$. The maximum of $f_p$ occurs at $x_0 = \frac{1}{\varepsilon \log p} - 1$. In this problem, we are interested in the integers, so we consider $b = \lfloor x_0 \rfloor$ and $c = \lceil x_0 \rceil$.

5.6.28 Let $f$ and $g$ be arithmetic functions such that $f = g * 1$. Suppose that $\sum_{n=1}^{\infty} \frac{g(n)}{n}$ converges absolutely. Show that

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} f(n) = \sum_{n=1}^{\infty} \frac{g(n)}{n}.$$

**Hint.** Follow the usual method. To estimate the error term, write

$$\sum_{d\leq x} |g(d)| = \sum_{d\leq\sqrt{x}} \frac{|g(d)|}{d} d + \sum_{\sqrt{x}<d\leq x} \frac{|g(d)|}{d} d.$$

5.6.29 Let $Q(x)$ be the number of squarefree positive integers less than or equal to $x$. Show that

$$Q(x) = \frac{6}{\pi^2} x + O(\sqrt{x}).$$

In general, show that if $Q_k(x)$ is the number of $k$th power free integers less than or equal to $x$, then

$$Q_k(x) = \frac{x}{\zeta(k)} + O\left(x^{1/k}\right), \quad \text{where } \zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}.$$

**Hint.** Recall that a positive integer $n$ is called $k$th power free if there is no prime $p$ such that $p^k \mid n$. In addition, $\sum_{d^2|n} \mu(d) = 1$ if $n$ is squarefree and is zero otherwise. Furthermore, $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$.

## Hints for Exercises 6.4

6.4.5 Prove the following statements by applying the prime number theorem.

(i) If $a > 0$ and $b > 0$, then $\pi(ax)/\pi(bx) \sim a/b$ as $x \to \infty$.

(ii) If $0 < a < b$, there exists an $x_0$ such that $\pi(ax) < \pi(bx)$ if $x \geq x_0$.

(iii) If $0 < a < b$, there exists an $x_0$ such that for $x \geq x_0$ there is at least one prime in the interval $(ax, bx]$.

**Hint.** If $\lim_{x\to\infty} f(x)$ exists and is less than 1, then we can show that there exists $x_0$ such that $f(x) < 1$ for all $x \geq x_0$.

6.4.6 If $0 < a < b$, show that the interval $(a, b)$ contains a rational number of the form $p/q$, where $p$ and $q$ are primes. (You can use the result from the previous exercise).

**Hint.** Suppose $0 < a < b$. Then there exists $c \in (a, b)$. Apply Exercise 6.4.3 to $\pi(ax)$ and $\pi(cx)$.

6.4.9 Let $A = \left\{n \in \mathbb{N} \mid \text{ there exists a prime } p \mid n \text{ such that } p > \sqrt{n}\right\}$, and let $A(x)$ be the number of the elements of $A$ that are $\leq x$.

(i) Show that $A(x) \gg \frac{x}{\log x}$ for $x \geq 2$.

(ii) Show that $\liminf_{x\to\infty} \frac{A(x)}{x} \geq \log 2$.

**Hint.** We observe that

$$A(x) = \sum_{\substack{n\leq x\\ \exists p|n\\ p>\sqrt{n}}} 1 \geq \sum_{\sqrt{x}<p\leq x} \sum_{\substack{n\leq x\\ p|n}} 1 = \sum_{\sqrt{x}<p\leq x} \left\lfloor \frac{x}{p} \right\rfloor.$$

6.4.13 Show that for all large $n$, we have

(i) $\sum_{d|n} \frac{1}{d} \ll \log\log n$,

(ii) $\sum_{p|n} \frac{1}{p} \ll \log\log\log n$.

**Hint.** The sum in (i) is $\sigma(n)/n$. For (ii), suppose $\omega(n) = k$ and $m = p_1 p_2 p_3 \cdots p_k$. Then $m \leq n$ and

$$\sum_{p|n} \frac{1}{p} \leq \sum_{p|m} \frac{1}{p}.$$

## Hints for Exercises 7.8

7.8.3 Let $f_1, \dots, f_m$ be the characters of a finite group $G$ of order $m$, and let $a$ be an element of $G$ of order $n$. Each number $f_r(a)$ is an $n$th root of unity. Prove that every $n$th root of unity occurs equally often among the numbers $f_1(a), f_2(a), \dots, f_m(a)$.

**Hint.** Evaluate the sum

$$\sum_{r=1}^{m} \sum_{k=1}^{n} f_r(a^k) e^{-2\pi i k/n}$$

in two ways to determine the number of times $e^{2\pi i/n}$ occurs. Since $f_r(a)$ is an $n$th root of unity, there is $c = 1, 2, \dots, n$ such that $f_r(a) = e(c/n)$. In addition,

$$\sum_{k=1}^{n} e\left(\frac{k(c-\ell)}{n}\right) = \begin{cases} n, & c \equiv \ell \pmod{n}; \\ 0, & \text{otherwise.} \end{cases}$$

Change the order of summation and apply Theorem 7.11 to evaluate the sum in the other way.

7.8.10 Show that there are arbitrarily long strings of consecutive integers that are not the sums of two squares.

**Hint.** Use the Chinese remainder theorem, a result of the sum of two squares in Chapter 1, and observe that if $n \equiv p \pmod{p^2}$, then $v_p(n) = 1$.

7.8.15 Let $a, q \in \mathbb{N}$ and $(a, q) = 1$. Dirichlet's theorem says that $A(a, q)$ contains infinitely many primes. This exercise gives a small extension of Dirichlet's theorem to other integer sequences related to primes.

(i) If $k \in \mathbb{N}$ is given, show that $A(a, q)$ contains infinitely many positive integers $n$ such that $\omega(n) = \Omega(n) = k$. In other words, $A(a, q)$ contains infinitely many squarefree integers having exactly $k$ prime factors.

(ii) A positive integer $n$ is called squarefull if $p^2 \mid n$ for every $p \mid n$. If $k \in \mathbb{N}$ is given, show that $A(a, q)$ contains infinitely many squarefull integers $n$ such that $\omega(n) = k$.

**Hint.** If $p \equiv a \pmod{q}$ and $p_1, p_2, \dots, p_{k-1} \equiv 1 \pmod{q}$, then $pp_1 \cdots p_{k-1} \equiv a \pmod{q}$. For (ii), if $p \equiv a \pmod{q}$, then $(p, q) = (a, q) = 1$ and $p^{m\varphi(q)+1} \equiv a \pmod{q}$.

7.8.20 Let $n$ and $k$ be positive integers. Show that there exists a set of $n$ consecutive integers such that each member of this set is divisible by $k$ distinct prime factors no one of which divides any other member of the set.

**Hint.** Use Exercise 7.8.19. Induction on $k$. Consider $n$ consecutive integers $(a_n!)^2 + a_1, (a_n!)^2 + a_2, \ldots, (a_n!)^2 + a_n$.

7.8.29 Let $g(n)$ be the length of longest arithmetic progressions of primes in $[1, n]$. Show that $g(n) \ll \log n$ for all $n \geq 2$.

**Hint.** Exercise 7.8.21 and Chebyshev's estimate.

7.8.30 For each arithmetic function $f$ and positive integer $k$, let

$$A(f, k) = \{n \in \mathbb{N} \mid f(n) \equiv 0 \pmod{k}\}.$$

Show that if $k \in \mathbb{N}$ is given and $f = d$, $\varphi$, or $\sigma$ (the divisor function, the Euler function, the sum of divisors function), then $A(f, k)$ contains an infinite arithmetic progression.

**Hint.** Apply Dirichlet's theorem and the lifting the exponent lemma. If $f = d$, consider $n = 2^{k-1}(2m + 1)$. If $f = \varphi$, let $n = k\gamma(k)m$ where $\gamma(k) = \prod_{p|k} p$. Suppose $f = \sigma$ and $k = 2^a p_1^{a_1} p_2^{a_2} \cdots p_\ell^{a_\ell}$. Choose the primes $q_0, q_1, \ldots, q_\ell$ satisfying $q_0 \equiv 1 \pmod{2}$ and $q_i \equiv 1 \pmod{p_i}$ for each $i \geq 1$. Let $n_0 = q_0^{b_0} q_1^{b_1} \cdots q_\ell^{b_\ell}$ and $n = n_0(1 + n_0 m)$ where the $b_i$ can be suitably chosen by the lifting the exponent lemma.

7.8.31 Prove that there exist arbitrarily long arithmetic progressions whose terms are powers of positive integers with integer exponent larger than 1. Show also that if $(a_n)_{n\geq 1}$ is an infinite arithmetic progression, then $(a_n)_{n\geq 1}$ contains a term which is not a perfect power.

**Hint.** Let $s$ be a positive integer. Let $p_n$ be the $n$th prime and let $M = p_1 p_2 p_3 \cdots p_s$. By the Chinese remainder theorem, for each $k = 1, 2, \ldots, s$, there exists a positive integer $a_k$ such that $a_k \equiv -1 \pmod{p_k}$ and $a_k \equiv 0 \pmod{\frac{M}{p_k}}$. Let $Q = \prod_{n=1}^{s} n^{a_n}$. For each $k = 1, 2, \ldots, s$, let

$$Q_k = k^{\frac{a_k+1}{p_k}} \prod_{\substack{n=1 \\ n\neq k}}^{s} n^{\frac{a_n}{p_k}}.$$

Show that $Q_k^{p_k} = kQ$.

## Hints for Exercises 8.7

8.7.2 Suppose $\sum_{n=1}^{\infty} f(n)n^{-s}$ converges at $s = s_0$. Show that the series converges uniformly on every compact subset of the half-plane $\sigma > \sigma_0$.

**Hint.** Take $H$ in Theorem 8.8 large.

8.7.7 Show that

(i) $B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$ for every $n \geq 0$,

(ii) $B_n = \sum_{k=0}^{n} \binom{n}{k} B_k$ for every $n \geq 2$.

**Hint.** Induction and Exercise 4.8.16. If (i) holds for $n$, then $B_{n+1}(x)$ is equal to

$$(n+1)\sum_{k=0}^{n} \binom{n}{k} B_k \frac{x^{n-k+1}}{n-k+1} + B_{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} B_k x^{n+1-k}.$$

8.7.10 Prove that the Bernoulli polynomials satisfy the following formulas:

(i) (Addition Formula) $B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x) y^{n-k}$,

(ii) (Multiplication Formula)

$$B_n(mx) = m^{n-1} \sum_{k=0}^{m-1} B_n\left(x + \frac{k}{m}\right).$$

**Hint.** For (i), recall the result in Exercise 4.8.10. To prove (ii), you may need to apply Theorem 4.19 for $0 < x < 1/m$ and then extend it by continuity to $0 \leq x \leq 1/m$. Let

$$f(x) = B_n(mx) - m^{n-1} \sum_{k=0}^{m-1} B_n\left(x + \frac{k}{m}\right).$$

Show that $f$ has period $1/m$.

8.7.11 Let $r \in \mathbb{N}$. Show that

$$\sum_{k=0}^{r} \frac{2^{2k} B_{2k}}{(2k)!\,(2r+1-2k)!} = \frac{1}{(2r)!}.$$

**Hint.** $B_n\left(\frac{1}{x}\right) - B_n\left(-\frac{1}{x}\right) = \sum_{k=0}^{n} \binom{n}{k} B_k \frac{1}{x^{n-k}} \left(1 - (-1)^{n-k}\right)$.

# Bibliography

[1] Boris Adamczewski and Yann Bugeaud, *Palindromic continued fractions* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **57** (2007), no. 5, 1557–1574. MR2364142

[2] Boris Adamczewski and Yann Bugeaud, *Transcendence measures for continued fractions involving repetitive or symmetric patterns*, J. Eur. Math. Soc. (JEMS) **12** (2010), no. 4, 883–914, DOI 10.4171/JEMS/218. MR2654083

[3] J. M. Aldaz, A. Bravo, S. Gutiérrez, and A. Ubis, *A theorem of D. J. Newman on Euler's $\phi$ function and arithmetic progressions*, Amer. Math. Monthly **108** (2001), no. 4, 364–367, DOI 10.2307/2695244. MR1836946

[4] K. Alladi and P. Erdős, *On an additive arithmetic function*, Pacific J. Math. **71** (1977), no. 2, 275–294. MR447086

[5] K. Alladi, P. Erdős, and V. E. Hoggatt Jr., *On additive partitions of integers*, Discrete Math. **22** (1978), no. 3, 201–211, DOI 10.1016/0012-365X(78)90053-5. MR522715

[6] Jean-Paul Allouche and Jeffrey Shallit, *Automatic sequences*, Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations, DOI 10.1017/CBO9780511546563. MR1997038

[7] Petr Ambrož, Zuzana Masáková, Edita Pelantová, and Christiane Frougny, *Palindromic complexity of infinite words associated with simple Parry numbers* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **56** (2006), no. 7, 2131–2160. Numération, pavages, substitutions. MR2290777

[8] Titu Andreescu and Dorin Andrica, *Number theory*, Birkhäuser Boston, Ltd., Boston, MA, 2009. Structures, examples, and problems, DOI 10.1007/b11856. MR2492316

[9] Titu Andreescu and Dorin Andrica, *Quadratic Diophantine equations*, Developments in Mathematics, vol. 40, Springer, New York, 2015. With a foreword by Preda Mihăilescu, DOI 10.1007/978-0-387-54109-9. MR3362224

[10] Titu Andreescu, Dorin Andrica, and Ion Cucurezeanu, *An introduction to Diophantine equations*, Birkhäuser Verlag, New York, 2010. A problem-based approach, DOI 10.1007/978-0-8176-4549-6. MR2723590

[11] George E. Andrews, *The theory of partitions*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1998. Reprint of the 1976 original. MR1634067

[12] George E. Andrews and Bruce C. Berndt, *Ramanujan's lost notebook. Part I*, Springer, New York, 2005. MR2135178

[13] George E. Andrews and Bruce C. Berndt, *Ramanujan's lost notebook. Part II*, Springer, New York, 2009. MR2474043

[14] George E. Andrews and Bruce C. Berndt, *Ramanujan's lost notebook. Part III*, Springer, New York, 2012, DOI 10.1007/978-1-4614-3810-6. MR2952081

[15] George E. Andrews and Bruce C. Berndt, *Ramanujan's lost notebook. Part IV*, Springer, New York, 2013

[16] Rodrigo Angelo, *A Cameron and Erdős conjecture on counting primitive sets*, Integers **18** (2018), Paper No. A25, 4. MR3783884

[17] Tom M. Apostol, *Mathematical analysis*, 2nd ed., Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1974. MR0344384

[18] Tom M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976. MR0434929

[19] Rafael Arce-Nazario, Francis N. Castro, and Raúl Figueroa, *On the equation* $\sum_{i=1}^{n} \frac{1}{x_i} = 1$ *in distinct odd or even numbers*, Contrib. Discrete Math. **11** (2017), no. 2, 63–78, DOI 10.3934/amc.2017025. MR3662290

[20] Saralee Aursukaree, Tammatada Khemaratchatakumthorn, and Prapanpong Pongsriiam, *Generalizations of Hermite's identity and applications*, Fibonacci Quart. **57** (2019), no. 2, 126–133. MR3957427

[21] Saralee Aursukaree and Prapanpong Pongsriiam, *On exactly 3-deficient-perfect numbers*, Fibonacci Quart. **59** (2021), no. 1, 33–46. MR4256585

[22] Mohamed Ayad and Omar Kihel, *On relatively prime sets*, Integers **9** (2009), A28, 343–352, DOI 10.1515/INTEG.2009.029. MR2592515

[23] Michael Baake, *A note on palindromicity*, Lett. Math. Phys. **49** (1999), no. 3, 217–227, DOI 10.1023/A:1007678316583. MR1743453

[24] P. Bachmann, *Zahlentheorie, II, Die analytische Zahlentheorie*, Leipzig: Teubner, 1894

[25] Mohamed El Bachraoui, *The number of relatively prime subsets and phi functions for* $\{m, m+1, \ldots, n\}$, Integers **7** (2007), A43, 8. MR2373105

[26] Mohamed El Bachraoui and Mohamed Salim, *Combinatorial identities involving the Möbius function*, J. Integer Seq. **13** (2010), no. 8, Article 10.8.6, 7. MR2718237

[27] Daniel Baczkowski, Michael Filaseta, Florian Luca, and Ognian Trifonov, *On values of* $d(n!)/m!$, $\phi(n!)/m!$ *and* $\sigma(n!)/m!$, Int. J. Number Theory **6** (2010), no. 6, 1199–1214, DOI 10.1142/S1793042110003435. MR2726578

[28] R. P. Bambah and S. Chowla, *On numbers which can be expressed as a sum of two squares*, Proc. Nat. Inst. Sci. India **13** (1947), 101–103. MR22879

[29] William D. Banks, *Every natural number is the sum of forty-nine palindromes*, Integers **16** (2016), Paper No. A3, 1–9. MR3458332

[30] William D. Banks, Derrick N. Hart, and Mayumi Sakata, *Almost all palindromes are composite*, Math. Res. Lett. **11** (2004), no. 5-6, 853–868, DOI 10.4310/MRL.2004.v11.n6.a10. MR2106245

[31] William D. Banks, Roger Heath-Brown, and Igor E. Shparlinski, *On the average value of divisor sums in arithmetic progressions*, Int. Math. Res. Not. **1** (2005), 1–25, DOI 10.1155/IMRN.2005.1. MR2130051

[32] William D. Banks and Igor E. Shparlinski, *Prime divisors of palindromes*, Period. Math. Hungar. **51** (2005), no. 1, 1–10, DOI 10.1007/s10998-005-0016-6. MR2180629

[33] William D. Banks and Igor E. Shparlinski, *Prime numbers with Beatty sequences*, Colloq. Math. **115** (2009), no. 2, 147–157, DOI 10.4064/cm115-2-1. MR2491740

[34] János Barát and Péter P. Varjú, *Partitioning the positive integers to seven Beatty sequences*, Indag. Math. (N.S.) **14** (2003), no. 2, 149–161, DOI 10.1016/S0019-3577(03)90000-0. MR2026810

[35] János Barát and Péter P. Varjú, *A contribution to infinite disjoint covering systems* (English, with English and French summaries), J. Théor. Nombres Bordeaux **17** (2005), no. 1, 51–55. MR2152210

[36] M. B. Barban, *The large sieve method and its applications in the theory of numbers*, Russian Math. Surveys **22** (1966), 49–103.

[37] Paul T. Bateman and Harold G. Diamond, *A hundred years of prime numbers*, Amer. Math. Monthly **103** (1996), no. 9, 729–741, DOI 10.2307/2974443. MR1416621

[38] Jonathan Bayless, Paul Kinlaw, and Dominic Klyve, *Sums over primitive sets with a fixed number of prime factors*, Math. Comp. **88** (2019), no. 320, 3063–3077, DOI 10.1090/mcom/3416. MR3985487

[39] Jonathan Bayless and Dominic Klyve, *Reciprocal sums as a knowledge metric: theory, computation, and perfect numbers*, Amer. Math. Monthly **120** (2013), no. 9, 822–831, DOI 10.4169/amer.math.monthly.120.09.822. MR3115443

[40] Samuel Beatty, *Problem 3173*, Amer. Math. Monthly **33** (1926), 159.

[41] Samuel Beatty, A. Ostrowski, J. Hyslop, and A. C. Aitken, *Problems and Solutions: Solutions: 3177*, Amer. Math. Monthly **34** (1927), no. 3, 159–160, DOI 10.2307/2298716. MR1521129

[42] Hacène Belbachir and Abdelkader Khelladi, *On a sum involving powers of reciprocals of an arithmetical progression*, Ann. Math. Inform. **34** (2007), 29–31. MR2385421

[43] Bruce C. Berndt, *Ramanujan's notebooks. Part I*, Springer-Verlag, New York, 1985. With a foreword by S. Chandrasekhar, DOI 10.1007/978-1-4612-1088-7. MR781125

[44] Bruce C. Berndt, *Ramanujan's notebooks. Part II*, Springer-Verlag, New York, 1989, DOI 10.1007/978-1-4612-4530-8. MR970033

[45] Bruce C. Berndt, *Ramanujan's notebooks. Part III*, Springer-Verlag, New York, 1991, DOI 10.1007/978-1-4612-0965-2. MR1117903

[46] Bruce C. Berndt, *Ramanujan's notebooks. Part IV*, Springer-Verlag, New York, 1994, DOI 10.1007/978-1-4612-0879-2. MR1261634

[47] Bruce C. Berndt, *Ramanujan's notebooks. Part V*, Springer-Verlag, New York, 1998, DOI 10.1007/978-1-4612-1624-7. MR1486573

[48] Bruce C. Berndt, Sun Kim, and Alexandru Zaharescu, *Weighted divisor sums and Bessel function series, II*, Adv. Math. **229** (2012), no. 3, 2055–2097, DOI 10.1016/j.aim.2011.10.016. MR2871168

[49] Bruce C. Berndt, Sun Kim, and Alexandru Zaharescu, *Circle and divisor problems, and double series of Bessel functions*, Adv. Math. **236** (2013), 24–59, DOI 10.1016/j.aim.2012.11.017. MR3019715

[50] Bruce C. Berndt, Sun Kim, and Alexandru Zaharescu, *The circle problem of Gauss and the divisor problem of Dirichlet—still unsolved*, Amer. Math. Monthly **125** (2018), no. 2, 99–114, DOI 10.1080/00029890.2018.1401853. MR3756337

[51] Bruce C. Berndt and Prapanpong Pongsriiam, *Discarded fragments from Ramanujan's papers*, Analytic and probabilistic methods in number theory, TEV, Vilnius, 2012, pp. 49–59. MR3025457

[52] A. S. Besicovitch, *On the density of certain sequences of integers*, Math. Ann. **110** (1935), no. 1, 336–341, DOI 10.1007/BF01448032. MR1512943

[53] Manjul Bhargava, *The factorial function and generalizations*, Amer. Math. Monthly **107** (2000), no. 9, 783–799, DOI 10.2307/2695734. MR1792411

[54] B. J. Birch, *Multiplicative functions with non-decreasing normal order*, J. London Math. Soc. **42** (1967), 149–151, DOI 10.1112/jlms/s1-42.1.149. MR202675

[55] V. Blomer, *The average value of divisor sums in arithmetic progressions*, Q. J. Math. **59** (2008), no. 3, 275–286, DOI 10.1093/qmath/ham044. MR2444061

[56] H. Bohr, *Address of Professor Harold Bohr*, Proc. Internat. Congr. Math. (Cambridge, 1950) vol 1, Amer. Math. Soc., Providence, R. I., 1952, 127–134.

[57] E. Bombieri, *On the large sieve*, Mathematika **12** (1965), 201–225, DOI 10.1112/S0025579300005313. MR197425

[58] Olivier Bordellès, *Arithmetic tales*, Universitext, Springer, London, 2012. Translated from the French by Véronique Bordellès, DOI 10.1007/978-1-4471-4096-2. MR2952910

[59] J. Bourgain, *Decoupling, exponential sums and the Riemann zeta function*, J. Amer. Math. Soc. **30** (2017), no. 1, 205–224, DOI 10.1090/jams/860. MR3556291

[60] J. Bourgain and N. Watt, *Mean square of zeta function, circle problem and divisor problem revisited*, preprint 2017 available at `arXiv:1709.04340`.

[61] S. Brlek, S. Hamel, M. Nivat, and C. Reutenauer, *On the palindromic complexity of infinite words*, Internat. J. Found. Comput. Sci. **15** (2004), no. 2, 293–306, DOI 10.1142/S012905410400242X. MR2071459

[62] Kenneth A. Brown, Scott M. Dunn, and Joshua Harrington, *Arithmetic progressions in the polygonal numbers*, Integers **12** (2012), Paper No. A43, 7. MR3083416

[63] Paul S. Bruckman and Peter G. Anderson, *Conjectures on the $Z$-densities of the Fibonacci sequence*, Fibonacci Quart. **36** (1998), no. 3, 263–271. MR1627443

[64] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek, *On Fibonacci numbers with few prime divisors*, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 2, 17–20. MR2126070

[65] H. M. Bui, Brian Conrey, and Matthew P. Young, *More than 41% of the zeros of the zeta function are on the critical line*, Acta Arith. **150** (2011), no. 1, 35–64, DOI 10.4064/aa150-1-3. MR2825573

[66] Peter Bundschuh and Ralf Bundschuh, *The sequence of Lucas numbers is not stable modulo 2 and 5*, Unif. Distrib. Theory **5** (2010), no. 2, 113–130. MR2781412

[67] Ralf Bundschuh and Peter Bundschuh, *Distribution of Fibonacci and Lucas numbers modulo $3^k$*, Fibonacci Quart. **49** (2011), no. 3, 201–210, DOI 10.1134/s0010952511020079. MR2833323

[68] W. Burnside, *A rapidly convergent series for $\log N!$*, Messenger Math. **46** (1917), 157–159.

[69] S. A. Burr, *On moduli for which the Fibonacci sequence contains a complete system of residues*, Fibonacci Quart. **9** (1971), no. 5, 497–504, 526. MR294238

[70] E. Busche, *Ueber die Function* (German), J. Reine Angew. Math. **106** (1890), 65–80, DOI 10.1515/crll.1890.106.65. MR1580215

[71] Yvonne Buttkewitz, Christian Elsholtz, Kevin Ford, and Jan-Christoph Schlage-Puchta, *A problem of Ramanujan, Erdős, and Kátai on the iterated divisor function*, Int. Math. Res. Not. IMRN **17** (2012), 4051–4061, DOI 10.1093/imrn/rnr175. MR2972548

[72] P. J. Cameron and P. Erdős, *On the number of sets of integers with various properties*, Number theory (Banff, AB, 1988), de Gruyter, Berlin, 1990, pp. 61–79. MR1106651

[73] L. Carlitz, *An arithmetic sum connected with the greatest integer function*, Norske Vid. Selsk. Forh. Trondheim **32** (1959), 24–30. MR0125055

[74] L. Carlitz, *Some arithmetic sums connected with the greatest integer function*, Math. Scand. **8** (1960), 59–64, DOI 10.7146/math.scand.a-10592. MR125056

[75] R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), no. 5, 232–238, DOI 10.1090/S0002-9904-1910-01892-9. MR1558896

[76] R. D. Carmichael, *On Composite Numbers $P$ Which Satisfy the Fermat Congruence $a^{P-1} \equiv 1 \bmod P$*, Amer. Math. Monthly **19** (1912), no. 2, 22–27, DOI 10.2307/2972687. MR1517641

[77] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. (2) **15** (1913/14), no. 1-4, 49–70, DOI 10.2307/1967798. MR1502459

[78] Charles E. Chace, *The divisor problem for arithmetic progressions with small modulus*, Acta Arith. **61** (1992), no. 1, 35–50, DOI 10.4064/aa-61-1-35-50. MR1153920

[79] Gerard J. Chang and Ko Wei Lih, *Polynomial representation of primes*, Tamkang J. Math. **8** (1977), no. 2, 197–198. MR556405

[80] FengJuan Chen, *On exactly $K$-deficient-perfect numbers*, Integers **19** (2019), Paper No. A37, 1–9. MR3997442

[81] Jing Run Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176. MR434997

[82] Timothy Chow, *A new characterization of the Fibonacci-free partition*, Fibonacci Quart. **29** (1991), no. 2, 174–180. MR1119406

[83] Timothy Y. Chow and Christopher D. Long, *Additive partitions and continued fractions*, Ramanujan J. **3** (1999), no. 1, 55–72, DOI 10.1023/A:1009813309003. MR1687033

[84] Javier Cilleruelo, Florian Luca, and Lewis Baxter, *Every positive integer is a sum of three palindromes*, Math. Comp. **87** (2018), no. 314, 3023–3055, DOI 10.1090/mcom/3221. MR3834696

[85] O. Cira and P. Smarandache, *Various Arithmetic Functions and Their Applications*, PONS asbl, 2016

[86] Todd Cochrane and Robert E. Dressler, *Consecutive triples of sums of two squares*, Arch. Math. (Basel) **49** (1987), no. 4, 301–304, DOI 10.1007/BF01210713. MR913160

[87] Peter Cohen, Katherine Cordwell, Alyssa Epstein, Chung-Hang Kwan, Adam Lott, and Steven J. Miller, *On near-perfect numbers*, Acta Arith. **194** (2020), no. 4, 341–366, DOI 10.4064/aa180821-11-10. MR4103276

[88] Alina Carmen Cojocaru and M. Ram Murty, *An introduction to sieve methods and their applications*, London Mathematical Society Student Texts, vol. 66, Cambridge University Press, Cambridge, 2006. MR2200366

[89] David Conlon, Jacob Fox, and Yufei Zhao, *The Green-Tao theorem: an exposition*, EMS Surv. Math. Sci. **1** (2014), no. 2, 249–282, DOI 10.4171/EMSS/6. MR3285854

[90] J. Brian Conrey, *More than two fifths of the zeros of the Riemann zeta function are on the critical line*, J. Reine Angew. Math. **399** (1989), 1–26, DOI 10.1515/crll.1989.399.1. MR1004130

[91] J. Brian Conrey, *The Riemann hypothesis*, Notices Amer. Math. Soc. **50** (2003), no. 3, 341–353. MR1954010

[92] J. Brian Conrey, *Riemann's hypothesis*, The legacy of Bernhard Riemann after one hundred and fifty years. Vol. I, Adv. Lect. Math. (ALM), vol. 35, Int. Press, Somerville, MA, 2016, pp. 107–190. MR3525915

[93] John B. Cosgrave and Karl Dilcher, *An introduction to Gauss factorials*, Amer. Math. Monthly **118** (2011), no. 9, 812–829, DOI 10.4169/amer.math.monthly.118.09.812. MR2854003

[94] John B. Cosgrave and Karl Dilcher, *Sums of reciprocals modulo composite integers*, J. Number Theory **133** (2013), no. 11, 3565–3577, DOI 10.1016/j.jnt.2013.04.016. MR3084287

[95] Paul Cubre and Jeremy Rouse, *Divisibility properties of the Fibonacci entry point*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3771–3785, DOI 10.1090/S0002-9939-2014-12269-6. MR3251719

[96] Michael James Dancs, *On a variance arising in the Gauss circle problem*, ProQuest LLC, Ann Arbor, MI, 2002. Thesis (Ph.D.)–The Pennsylvania State University. MR2703841

[97] H. Davenport, *On the Addition of Residue Classes*, J. London Math. Soc. **10** (1935), no. 1, 30–32, DOI 10.1112/jlms/s1-10.37.30. MR1581695

[98] Harold Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000. Revised and with a preface by Hugh L. Montgomery. MR1790423

[99] H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities*, 2nd ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2005. With a foreword by R. C. Vaughan, D. R. Heath-Brown and D. E. Freeman; Edited and prepared for publication by T. D. Browning, DOI 10.1017/CBO9780511542893. MR2152164

[100] H. Davenport and H. Halberstam, *Primes in arithmetic progressions*, Michigan Math. J. **13** (1966), 485–489. MR200257

[101] Hubert Delange, *Sur les fonctions arithmétiques multiplicatives* (French), Ann. Sci. École Norm. Sup. (3) **78** (1961), 273–304. MR0169829

[102] Jean-Marie De Koninck and Florian Luca, *Analytic number theory*, Graduate Studies in Mathematics, vol. 134, American Mathematical Society, Providence, RI, 2012. Exploring the anatomy of integers, DOI 10.1090/gsm/134. MR2919246

[103] L. E. Dickson, *History of the Theory of Numbers Volume I Divisibility and Primality*, Dover Publications, 2005

[104] Domotorp, Is there an arbitrarily long arithmetic progression whose members are palindromes? A Question on MathOverflow (2015), available online at `https://mathoverflow.net/questions/206151/is-there-an-arbitrarily-long-arithmetic-progression-whose-members-are-palindrome`

[105] François G. Dorais and Dominic Klyve, *A Wieferich prime search up to* $6.7 \times 10^{15}$, J. Integer Seq. **14** (2011), no. 9, Article 11.9.2, 14. MR2859986

[106] Xavier Droubay and Giuseppe Pirillo, *Palindromes and Sturmian words*, Theoret. Comput. Sci. **223** (1999), no. 1-2, 73–85, DOI 10.1016/S0304-3975(97)00188-6. MR1704637

[107] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[108] Pierre Dusart, *Explicit estimates of some functions over primes*, Ramanujan J. **45** (2018), no. 1, 227–251, DOI 10.1007/s11139-016-9839-4. MR3745073

[109] G. Eisenstein, *Geometrischer Beweis des Fundamentaltheorems für die quadratischer Reste* (German), J. Reine Angew. Math. **28** (1844), 246–248, DOI 10.1515/crll.1844.28.246. MR1578429

[110] Peter D. T. A. Elliott, *Probabilistic number theory. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 239, Springer-Verlag, New York-Berlin, 1979. Mean-value theorems. MR551361

[111] Peter D. T. A. Elliott, *Probabilistic number theory. II*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 240, Springer-Verlag, Berlin-New York, 1980. Central limit theorems. MR560507

[112] Christian Elsholtz and Terence Tao, *Counting the number of solutions to the Erdős-Straus equation on unit fractions*, J. Aust. Math. Soc. **94** (2013), no. 1, 50–105, DOI 10.1017/S1446788712000468. MR3101397

[113] Christian Elsholtz, Marc Technau, and Niclas Technau, *The maximal order of iterated multiplicative functions*, Mathematika **65** (2019), no. 4, 990–1009, DOI 10.1112/s0025579319000214. MR3992359

[114] Paul Erdös, *Note on Sequences of Integers No One of Which is Divisible By Any Other*, J. London Math. Soc. **10** (1935), no. 2, 126–128, DOI 10.1112/jlms/s1-10.1.126. MR1574239

[115] Paul Erdös, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 374–384, DOI 10.1073/pnas.35.7.374. MR29411

[116] Paul Erdös, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206. MR79031

[117] Paul Erdős, S. W. Graham, Aleksandar Ivić, and Carl Pomerance, *On the number of divisors of* $n!$, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), Progr. Math., vol. 138, Birkhäuser Boston, Boston, MA, 1996, pp. 337–355. MR1399347

[118] Paul Erdős and I. Kátai, *On the growth of* $d_k(n)$, Fibonacci Quart. **7** (1969), 267–274. MR252338

[119] Paul Erdös and R. Obláth, *Über diophantische Gleichungen der Form* $n! = x^p \pm y^p$ *und* $n! \pm m! = x^p$, Acta Litt. Sci. Univ., Szeged **8** (1937), 241–255.

[120] Shaoji Feng, *Zeros of the Riemann zeta function on the critical line*, J. Number Theory **132** (2012), no. 4, 511–542, DOI 10.1016/j.jnt.2011.10.002. MR2887604

[121] Gabriele Fici and Luca Q. Zamboni, *On the least number of palindromes contained in an infinite word*, Theoret. Comput. Sci. **481** (2013), 1–8, DOI 10.1016/j.tcs.2013.02.013. MR3037792

[122] Steven R. Finch, *Mathematical constants*, Encyclopedia of Mathematics and its Applications, vol. 94, Cambridge University Press, Cambridge, 2003. MR2003519

[123] Nathan J. Fine, *Basic hypergeometric series and applications*, Mathematical Surveys and Monographs, vol. 27, American Mathematical Society, Providence, RI, 1988. With a foreword by George E. Andrews, DOI 10.1090/surv/027. MR956465

[124] Stéphane Fischler, *Palindromic prefixes and Diophantine approximation*, Monatsh. Math. **151** (2007), no. 1, 11–37, DOI 10.1007/s00605-006-0425-5. MR2317388

[125] Étienne Fouvry and Henryk Iwaniec, *The divisor function over arithmetic progressions*, Acta Arith. **61** (1992), no. 3, 271–287, DOI 10.4064/aa-61-3-271-287. With an appendix by Nicholas Katz. MR1161479

[126] Aviezri S. Fraenkel, *The bracket function and complementary sets of integers*, Canadian J. Math. **21** (1969), 6–27, DOI 10.4153/CJM-1969-002-7. MR234900

[127] Aviezri S. Fraenkel, *Complementing and exactly covering sequences*, J. Combinatorial Theory Ser. A **14** (1973), 8–20, DOI 10.1016/0097-3165(73)90059-9. MR309770

[128] Aviezri S. Fraenkel, *Complementary systems of integers*, Amer. Math. Monthly **84** (1977), no. 2, 114–115, DOI 10.2307/2319931. MR429815

[129] Aviezri S. Fraenkel, *How to beat your Wythoff games' opponent on three fronts*, Amer. Math. Monthly **89** (1982), no. 6, 353–361, DOI 10.2307/2321643. MR660914

[130] Aviezri S. Fraenkel, *Wythoff games, continued fractions, cedar trees and Fibonacci searches*, Theoret. Comput. Sci. **29** (1984), no. 1-2, 49–73, DOI 10.1016/0304-3975(84)90012-4. MR742402

[131] Aviezri S. Fraenkel, *Heap games, numeration systems and sequences*, Ann. Comb. **2** (1998), no. 3, 197–210, DOI 10.1007/BF01608532. MR1681514

[132] G. A. Freĭman, *Foundations of a structural theory of set addition*, Translations of Mathematical Monographs, Vol 37, American Mathematical Society, Providence, R.I., 1973. Translated from the Russian. MR0360496

[133] A. E. Frid, S. Puzynina, and L. Q. Zamboni, *On palindromic factorization of words*, Adv. in Appl. Math. **50** (2013), no. 5, 737–748, DOI 10.1016/j.aam.2013.01.002. MR3044569

[134] Anna E. Frid, *Sturmian numeration systems and decompositions to palindromes*, European J. Combin. **71** (2018), 202–212, DOI 10.1016/j.ejc.2018.04.003. MR3802244

[135] John B. Friedlander and D. A. Goldston, *Variance of distribution of primes in residue classes*, Quart. J. Math. Oxford Ser. (2) **47** (1996), no. 187, 313–336, DOI 10.1093/qmath/47.3.313. MR1412558

[136] John B. Friedlander and Henryk Iwaniec, *The divisor problem for arithmetic progressions*, Acta Arith. **45** (1985), no. 3, 273–277, DOI 10.4064/aa-45-3-273-277. MR808026

[137] John B. Friedlander and Henryk Iwaniec, *Incomplete Kloosterman sums and a divisor problem*, Ann. of Math. (2) **121** (1985), no. 2, 319–350, DOI 10.2307/1971175. With an appendix by Bryan J. Birch and Enrico Bombieri. MR786351

[138] John Friedlander and Henryk Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications, vol. 57, American Mathematical Society, Providence, RI, 2010, DOI 10.1090/coll/057. MR2647984

[139] P. X. Gallagher, *The large sieve*, Mathematika **14** (1967), 14–20, DOI 10.1112/S0025579300007968. MR214562

[140] P. X. Gallagher, *Bombieri's mean value theorem*, Mathematika **15** (1968), 1–6, DOI 10.1112/S002557930000231X. MR237442

[141] C. F. Gauss, *Commentationes societatis regiae scientiarum gottingensis 16* (*1808*), Göttingen; also Werke, Göttingen, 1876, Band 2, 1–8.

[142] A. O. Gelfond and Yu. V. Linnik, *Elementary methods in analytic number theory*, Rand McNally & Co., Chicago, Ill., 1965. Translated by Amiel Feinstein; Revised and edited by L. J. Mordell. MR0188135

[143] D. Goldfeld, *The elementary proof of the prime number theorem: an historical perspective*, Number theory (New York, 2003), Springer, New York, 2004, pp. 179–192. MR2044518

[144] D. Goldfeld: *The elementary proof of the prime number theorem: An historical perspective*, `https://www.math.columbia.edu/~goldfeld/ErdosSelbergDispute.pdf`

[145] Daniel A. Goldston, János Pintz, and Cem Y. Yıldırım, *Primes in tuples. I*, Ann. of Math. (2) **170** (2009), no. 2, 819–862, DOI 10.4007/annals.2009.170.819. MR2552109

[146] Daniel A. Goldston and R. C. Vaughan, *On the Montgomery-Hooley asymptotic formula*, Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), London Math. Soc. Lecture Note Ser., vol. 237, Cambridge Univ. Press, Cambridge, 1997, pp. 117–142, DOI 10.1017/CBO9780511526091.010. MR1635742

[147] Lee M. Goswick, Emil W. Kiss, Gábor Moussong, and Nándor Simányi, *Sums of squares and orthogonal integral vectors*, J. Number Theory **132** (2012), no. 1, 37–53, DOI 10.1016/j.jnt.2011.07.001. MR2843297

[148] Ronald L. Graham, *A theorem on partitions*, J. Austral. Math. Soc. **3** (1963), 435–441. MR0162760

[149] Ronald L. Graham, *On finite sums of reciprocals of distinct $n$th powers*, Pacific J. Math. **14** (1964), 85–92. MR159788

[150] Ronald L. Graham, *On finite sums of unit fractions*, Proc. London Math. Soc. (3) **14** (1964), 193–207, DOI 10.1112/plms/s3-14.2.193. MR160757

[151] Ronald L. Graham, *Covering the positive integers by disjoint sets of the form* $\{[n\alpha + \beta] : n = 1, 2, \ldots\}$, J. Combinatorial Theory Ser. A **15** (1973), 354–358, DOI 10.1016/0097-3165(73)90084-8. MR325564

[152] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, 2nd ed., Addison-Wesley Publishing Company, Reading, MA, 1994. A foundation for computer science. MR1397498

[153] Andrew Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253–276. MR1483922

[154] A. Granville, *Arithmetic properties of binomial coefficients: a dynamic survey*, available at `http://www.dms.umontreal.ca/~andrew/Binomial/`

[155] Andrew Granville, *Prime number patterns*, Amer. Math. Monthly **115** (2008), no. 4, 279–296, DOI 10.1080/00029890.2008.11920529. MR2398409

[156] Hester Graves and M. Ram Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, J. Number Theory **133** (2013), no. 6, 1809–1813, DOI 10.1016/j.jnt.2012.10.012. MR3027939

[157] Great Internet Mersenne Prime Search (GIMPS), `http://www.mersenne.org/`

[158] Ben Green, *Long arithmetic progressions of primes*, Analytic number theory, Clay Math. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 2007, pp. 149–167. MR2362199

[159] Ben Green and Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547, DOI 10.4007/annals.2008.167.481. MR2415379

[160] Robert E. Greene and Steven G. Krantz, *Function theory of one complex variable*, 2nd ed., Graduate Studies in Mathematics, vol. 40, American Mathematical Society, Providence, RI, 2002, DOI 10.1090/gsm/040. MR1871333

[161] R. C. Grimson, *The evaluation of a sum of Jacobsthal*, Norske Vid. Selsk. Skr. (Trondheim) **4** (1974), 6. MR371795

[162] E. Grosswald, A. Calloway, and J. Calloway, *The representation of integers by three positive squares*, Proc. Amer. Math. Soc. **10** (1959), 451–455, DOI 10.2307/2032865. MR104623

[163] N. H. Guersenzvaig and M. Z. Spivey, *Some inversion formulas for sums of quotients*, Crux Mathematicorum, **32**(1) (2006), 39–43.

[164] Richard K. Guy, *Unsolved problems in number theory*, 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004, DOI 10.1007/978-0-387-26677-0. MR2076335

[165] Jacob Hacks, *Über Summen von Grössten Ganzen* (German), Acta Math. **10** (1887), no. 1, 1–52, DOI 10.1007/BF02393691. MR1554726

[166] R. D. Haertel, *Summation formulas for the greatest integer part function*, Master thesis, Oregon State University, 1964

[167] Heini Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, No. 4, Academic Press [Harcourt Brace Jovanovich, Publishers], London-New York, 1974. MR0424730

[168] Heini Halberstam and Klaus Friedrich Roth, *Sequences*, 2nd ed., Springer-Verlag, New York-Berlin, 1983. MR687978

[169] F. David Hammer, J. C. Binz, and James Propp, *Problems and Solutions: Solutions of Elementary Problems: E3010*, Amer. Math. Monthly **95** (1988), no. 2, 133–134, DOI 10.2307/2323071. MR1541255

[170] Denis Hanson, *On the product of the primes*, Canad. Math. Bull. **15** (1972), 33–37, DOI 10.4153/CMB-1972-007-7. MR313179

[171] G. H. Hardy, *Orders of Infinity*, Cambridge Tract 12, Cambridge University Press, 1910

[172] G. H. Hardy, *Sur les zéros de la fonction* $\zeta(s)$ *de Riemann*, C. R. Acad. Sci. Paris, **158** (1914), 1012–1014; Collected Papers, Vol. 2, Oxford: Oxford University Press, 1967, pp. 6–8.

[173] G. H. Hardy, *On Dirichlet's Divisor Problem*, Proc. London Math. Soc. (2) **15** (1916), 1–25, DOI 10.1112/plms/s2-15.1.1. MR1576550

[174] G. H. Hardy and J. E. Littlewood, *Some problems of diophantine approximation*, Acta Math. **37** (1914), no. 1, 193–239, DOI 10.1007/BF02401834. MR1555099

[175] G. H. Hardy and J. E. Littlewood, *Contributions to the theory of the riemann zeta-function and the theory of the distribution of primes*, Acta Math. **41** (1916), no. 1, 119–196, DOI 10.1007/BF02422942. MR1555148

[176] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number $n$*, Quart. J. Math. **48** (1917), 76–92.

[177] G. H. Hardy and S. Ramanujan, *Asymptotic Formulaae in Combinatory Analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115, DOI 10.1112/plms/s2-17.1.75. MR1575586

[178] G. H. Hardy and M. Riesz, *The general theory of Dirichlet's series*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 18, Stechert-Hafner, Inc., New York, 1964. MR0185094

[179] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, Oxford, 2008. Revised by D. R. Heath-Brown and J. H. Silverman; With a foreword by Andrew Wiles. MR2445243

[180] Glyn Harman, *Primes in Beatty sequences in short intervals*, Mathematika **62** (2016), no. 2, 572–586, DOI 10.1112/S0025579315000376. MR3521342

[181] Matúš Harminc and Roman Soták, *Palindromic numbers in arithmetic progressions*, Fibonacci Quart. **36** (1998), no. 3, 259–262. MR1627447

[182] Mehdi Hassani, *Factorization of factorials and a result of Hardy and Ramanujan*, Math. Inequal. Appl. **15** (2012), no. 2, 403–407, DOI 10.7153/mia-15-34. MR2962243

[183] D. R. Heath-Brown, *The divisor function $d_3(n)$ in arithmetic progressions*, Acta Arith. **47** (1986), no. 1, 29–56, DOI 10.4064/aa-47-1-29-56. MR866901

[184] Harald A. Helfgott, *The ternary Goldbuch problem*, preprint, 2015, available at https://arxiv.org/abs/1501.05438.

[185] A. J. Hildebrand, Xiaomin Li, Junxian Li, and Yun Xie, *Almost Beatty partitions*, J. Integer Seq. **22** (2019), no. 4, Art. 19.4.6, 34. MR4001006

[186] Adolf Hildebrand and Gérald Tenenbaum, *On the number of prime factors of an integer*, Duke Math. J. **56** (1988), no. 3, 471–501, DOI 10.1215/S0012-7094-88-05620-7. MR948530

[187] Michael D. Hirschhorn and Mark B. Villarino, *A refinement of Ramanujan's factorial approximation*, Ramanujan J. **34** (2014), no. 1, 73–81, DOI 10.1007/s11139-013-9494-y. MR3210256

[188] A. Hof, O. Knill, and B. Simon, *Singular continuous spectrum for palindromic Schrödinger operators*, Comm. Math. Phys. **174** (1995), no. 1, 149–159. MR1372804

[189] V. E. Hoggatt Jr., *Additive partitions of the positive integers*, Fibonacci Quart. **18** (1980), no. 3, 220–226. MR599653

[190] V. E. Hoggatt Jr. and Marjorie Bicknell-Johnson, *Additive partitions of the positive integers and generalized Fibonacci representations*, Fibonacci Quart. **22** (1984), no. 1, 2–21. MR734227

[191] Christopher Hooley, *On the intervals between numbers that are sums of two squares. II*, J. Number Theory **5** (1973), 215–217, DOI 10.1016/0022-314X(73)90046-2. MR325557

[192] Christopher Hooley, *On the intervals between numbers that are sums of two squares. III*, J. Reine Angew. Math. **267** (1974), 207–218. MR342479

[193] Christopher Hooley, *On the Barban-Davenport-Halberstam theorem. I*, J. Reine Angew. Math. **274(275)** (1975), 206–223, DOI 10.1515/crll.1975.274-275.206. MR382202

[194] Christopher Hooley, *On the Barban-Davenport-Halberstam theorem. II*, J. London Math. Soc. (2) **9** (1974/75), 625–636, DOI 10.1112/jlms/s2-9.4.625. MR382203

[195] Christopher Hooley, *On the Barban-Davenport-Halberstam theorem. III*, J. London Math. Soc. (2) **10** (1975), 249–256, DOI 10.1112/jlms/s2-10.2.249. MR382204

[196] Christopher Hooley, *On the Barban-Davenport-Halberstam theorem. IV*, J. London Math. Soc. (2) **11** (1975), no. 4, 399–407, DOI 10.1112/jlms/s2-11.4.399. MR382205

[197] C. Hooley, *On the Barban-Davenport-Halberstam theorem. IX*, Acta Arith. **83** (1998), no. 1, 17–30, DOI 10.4064/aa-83-1-17-30. MR1489564

[198] Christopher Hooley, *On the Barban-Davenport-Halberstam theorem. X*, Hardy-Ramanujan J. **21** (1998), 9 pp. MR1680125

[199] Christopher Hooley, *On the Barban-Davenport-Halberstam theorem. XIV*, Acta Arith. **101** (2002), no. 3, 247–292, DOI 10.4064/aa101-3-5. MR1875843

[200] Christopher Hooley, *On the Barban-Davenport-Halberstam theorem. XVIII*, Illinois J. Math. **49** (2005), no. 2, 581–643. MR2164354

[201] Christopher Hooley, *On the Barban-Davenport Halberstam theorem. XIX*, Hardy-Ramanujan J. **30** (2007), 56–67. MR2440321

[202] Loo Keng Hua, *Additive theory of prime numbers*, Translations of Mathematical Monographs, Vol. 13, American Mathematical Society, Providence, R.I., 1965. MR0194404

[203] Loo Keng Hua, *Introduction to number theory*, Springer-Verlag, Berlin-New York, 1982. Translated from the Chinese by Peter Shiu. MR665428

[204] M. N. Huxley, *Exponential sums and lattice points. II*, Proc. London Math. Soc. (3) **66** (1993), no. 2, 279–301, DOI 10.1112/plms/s3-66.2.279. MR1199067

[205] M. N. Huxley, *Exponential sums and lattice points. III*, Proc. London Math. Soc. (3) **87** (2003), no. 3, 591–609, DOI 10.1112/S0024611503014485. MR2005876

[206] M. N. Huxley, *The distribution of prime numbers*, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1972. Large sieves and zero-density theorems. MR0444593

[207] Karl-Heinz Indlekofer, *Scharfe untere Abschätzung für die Anzahlfunktion der B-Zwillinge* (German), Acta Arith. **26** (1974/75), 207–212, DOI 10.4064/aa-26-2-207-212. MR354586

[208] S. Ikehara, *An extension of Landau's theorem in the analytic theory of numbers*, J. Math. Phys. **10** (1931), 1–12.

[209] A. E. Ingham, *The distribution of prime numbers*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990. Reprint of the 1932 original; With a foreword by R. C. Vaughan. MR1074573

[210] Kenneth E. Iverson, *A programming language*, John Wiley & Sons, Inc., New York-London, 1962. MR0143354

[211] Aleksandar Ivić, *The Riemann zeta-function*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1985. The theory of the Riemann zeta-function with applications. MR792089

[212] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004, DOI 10.1090/coll/053. MR2061214

[213] Henryk Iwaniec and C. J. Mozzochi, *On the divisor and circle problems*, J. Number Theory **29** (1988), no. 1, 60–93, DOI 10.1016/0022-314X(88)90093-5. MR938870

[214] Eliot T. Jacobson, *Distribution of the Fibonacci numbers mod* $2^k$, Fibonacci Quart. **30** (1992), no. 3, 211–215. MR1175305

[215] Ernst Jacobsthal, *Über eine zahlentheoretische Summe* (German), Norske Vid. Selsk. Forh., Trondheim **30** (1957), 35–41. MR0090597

[216] Montree Jaidee and Prapanpong Pongsriiam, *Arithmetic functions of Fibonacci and Lucas numbers*, Fibonacci Quart. **57** (2019), no. 3, 246–254. MR3997072

[217] Lenny Jones and Tristan Phillips, *Arithmetic progressions of polygonal numbers with common difference a polygonal number*, Integers **17** (2017), Paper No. A43, 8. MR3708294

[218] Sutasinee Kawsumarng, Tammatada Khemaratchatakumthorn, Passawan Noppakaew, and Prapanpong Pongsriiam, *Sumsets associated with Wythoff sequences and Fibonacci numbers*, Period. Math. Hungar. **82** (2021), no. 1, 98–113, DOI 10.1007/s10998-020-00343-0. MR4219408

[219] Rizwanur Khan, *The divisor function in arithmetic progressions modulo prime powers*, Mathematika **62** (2016), no. 3, 898–908, DOI 10.1112/S0025579316000024. MR3521360

[220] Narissara Khaochim and Prapanpong Pongsriiam, *On the order of appearance of products of Fibonacci numbers*, Contrib. Discrete Math. **13** (2018), no. 2, 45–62, DOI 10.12988/ijcms.2018.812. MR3897223

[221] N. Khaochim and P. Pongsriiam, *The general case on the order of appearance of product of consecutive Lucas numbers*, Acta Math. Univ. Comenian. (N.S.) **87** (2018), no. 2, 277–289. MR3847356

[222] Daejun Kim, Jeongwon Lee, and Byeong-Kweon Oh, *A sum of three nonzero triangular numbers*, Int. J. Number Theory **17** (2021), no. 10, 2279–2300, DOI 10.1142/S1793042121500883. MR4322834

[223] Clark Kimberling, *Complementary equations and Wythoff sequences*, J. Integer Seq. **11** (2008), no. 3, Article 08.3.3, 8. MR2429960

[224] Clark Kimberling, *Beatty sequences and Wythoff sequences, generalized*, Fibonacci Quart. **49** (2011), no. 3, 195–200. MR2833322

[225] Paul Kinlaw, *Lower bounds for numbers with three prime factors*, Integers **19** (2019), Paper No. A22, 18. MR3928560

[226] Paul Kinlaw, Mitsuo Kobayashi, and Carl Pomerance, *On the equation* $\varphi(n) = \varphi(n+1)$, Acta Arith. **196** (2020), no. 1, 69–92, DOI 10.4064/aa190627-20-1. MR4129972

[227] Jiří Klaška, *Donald Dines Wall's conjecture*, Fibonacci Quart. **56** (2018), no. 1, 43–51. MR3782966

[228] M. Klazar, *Birch's theorem: if* $f(n)$ *is multiplicative and has a non-decreasing normal order then* $f(n) = n^\alpha$, available at `https://kam.mff.cuni.cz/~klazar/birch_thm`

[229] J. Korevaar, *On Newman's quick way to the prime number theorem*, Math. Intelligencer **4** (1982), no. 3, 108–115, DOI 10.1007/BF03024240. MR684025

[230] Thomas Koshy, *Fibonacci and Lucas numbers with applications*, Pure and Applied Mathematics (New York), Wiley-Interscience, New York, 2001, DOI 10.1002/9781118033067. MR1855020

[231] Bryna Kra, *The Green-Tao theorem on arithmetic progressions in the primes: an ergodic point of view*, Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 1, 3–23, DOI 10.1090/S0273-0979-05-01086-4. MR2188173

[232] J. Krandel and W. Chen, *Interpolating classical partitions of the set of positive integers*, Ramanujan J. (2020) available online at `https://doi.org/10.1007/s11139-019-00196-3`

[233] Jeffrey M. Kubina and Marvin C. Wunderlich, *Extending Waring's conjecture to* $471,600,000$, Math. Comp. **55** (1990), no. 192, 815–820, DOI 10.2307/2008448. MR1035936

[234] K. Kuhapatanakul and P. Ruankong, *Sums of square roots*, Math. Gaz. **101**(552) (2017), 476–480.

[235] Lawrence Kuipers and Jau Shyong Shiue, *A distribution property of the sequence of Fibonacci numbers*, Fibonacci Quart. **10** (1972), no. 4, 375–376, 392. MR314750

[236] J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* $2/3$, Pacific J. Math. **118** (1985), no. 2, 449–461. MR789184

[237] J. C. Lagarias, *Errata to: "The set of primes dividing the Lucas numbers has density* $2/3$*"* [*Pacific J. Math.* **118** (*1985*)*, no. 2, 449–461; MR0789184* (*86i:11007*)], Pacific J. Math. **162** (1994), no. 2, 393–396. MR1251907

[238] Edmund Landau, *Sur quelques problèmes relatifs à la distribution des nombres premiers* (French), Bull. Soc. Math. France **28** (1900), 25–38. MR1504359

[239] Edmund Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. und Physik **13** (1908), 305–312.

[240] Edmund Landau, *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände* (German), Chelsea Publishing Co., New York, 1953. 2d ed; With an appendix by Paul T. Bateman. MR0068565

[241] Reinhard C. Laubenbacher and David J. Pengelley, *Gauss, Eisenstein, and the "third" proof of the quadratic reciprocity theorem: Ein kleines Schauspiel*, Math. Intelligencer **16** (1994), no. 2, 67–72, DOI 10.1007/BF03024287. MR1270844

[242] Reinhard C. Laubenbacher and David J. Pengelley, *Gauss, Eisenstein, and the "third" proof of the quadratic reciprocity theorem: Ein kleines Schauspiel*, Math. Intelligencer **16** (1994), no. 2, 67–72, DOI 10.1007/BF03024287. MR1270844

[243] Norman Levinson, *More than one third of zeros of Riemann's zeta-function are on $\sigma = 1/2$*, Advances in Math. **13** (1974), 383–436, DOI 10.1016/0001-8708(74)90074-7. MR564081

[244] Jared Duker Lichtman, *The reciprocal sum of primitive nondeficient numbers*, J. Number Theory **191** (2018), 104–118, DOI 10.1016/j.jnt.2018.03.021. MR3825463

[245] Jared Duker Lichtman, *Microthesis: the Erdős primitive set conjecture*, Lond. Math. Soc. Newsl. **489** (2020), 33–34. MR4508972

[246] Jared Duker Lichtman and Carl Pomerance, *The Erdős conjecture for primitive sets*, Proc. Amer. Math. Soc. Ser. B **6** (2019), 1–14, DOI 10.1090/bproc/40. MR3937344

[247] Kui Liu, Igor E. Shparlinski, and Tianping Zhang, *Divisor problem in arithmetic progressions modulo a prime power*, Adv. Math. **325** (2018), 459–481, DOI 10.1016/j.aim.2017.12.006. MR3742595

[248] Aldo de Luca, *Sturmian words: structure, combinatorics, and their arithmetics*, Theoret. Comput. Sci. **183** (1997), no. 1, 45–82, DOI 10.1016/S0304-3975(96)00310-6. MR1468450

[249] Florian Luca, *Arithmetic functions of Fibonacci numbers*, Fibonacci Quart. **37** (1999), no. 3, 265–268. MR1709533

[250] Florian Luca, *Equations involving arithmetic functions of factorials* (English, with English and Spanish summaries), Divulg. Mat. **8** (2000), no. 1, 15–23. MR1762233

[251] Florian Luca, *Palindromes in various sequences* (Spanish, with Spanish summary), Gac. R. Soc. Mat. Esp. **20** (2017), no. 1, 49–56. MR3638677

[252] Florian Luca and Carl Pomerance, *On the local behavior of the order of appearance in the Fibonacci sequence*, Int. J. Number Theory **10** (2014), no. 4, 915–933, DOI 10.1142/S1793042114500079. MR3208867

[253] Florian Luca and Igor E. Shparlinski, *Arithmetic properties of the Ramanujan function*, Proc. Indian Acad. Sci. Math. Sci. **116** (2006), no. 1, 1–8, DOI 10.1007/BF02829735. MR2210301

[254] Florian Luca and Paul Thomas Young, *On the number of divisors of $n!$ and of the Fibonacci numbers*, Glas. Mat. Ser. III **47(67)** (2012), no. 2, 285–293, DOI 10.3336/gm.47.2.05. MR3006627

[255] D. Mackenzie and B. Cipra, *What's Happening in the Mathematical Sciences*, Volume 10, American Mathematical Society, 2016

[256] K. Mahler, *On the fractional parts of the powers of a rational number. II*, Mathematika **4** (1957), 122–124, DOI 10.1112/S0025579300001170. MR93509

[257] A. Mąkowski, *Three consecutive integers cannot be powers*, Colloq. Math. **9** (1962), 297. MR142504

[258] Henry B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. of Math. (2) **43** (1942), 523–527, DOI 10.2307/1968807. MR6748

[259] Diego Marques, *The Fibonacci version of the Brocard-Ramanujan Diophantine equation*, Port. Math. **68** (2011), no. 2, 185–189, DOI 10.4171/PM/1887. MR2849854

[260] Diego Marques, *The order of appearance of powers of Fibonacci and Lucas numbers*, Fibonacci Quart. **50** (2012), no. 3, 239–245. MR2981180

[261] Diego Marques, *The order of appearance of integers at most one away from Fibonacci numbers*, Fibonacci Quart. **50** (2012), no. 1, 36–43. MR2892008

[262] Diego Marques, *The order of appearance of product of consecutive Fibonacci numbers*, Fibonacci Quart. **50** (2012), no. 2, 132–139. MR2927931

[263] Diego Marques, *The order of appearance of the product of consecutive Lucas numbers*, Fibonacci Quart. **51** (2013), no. 1, 38–43. MR3029380

[264] Diego Marques and Pavel Trojovský, *The order of appearance of the product of five consecutive Lucas numbers*, Tatra Mt. Math. Publ. **59** (2014), 65–77, DOI 10.2478/tmmp-2014-0019. MR3332278

[265] Greg Martin, *The smallest solution of $\phi(30n+1) < \phi(30n)$ is ...*, Amer. Math. Monthly **106** (1999), no. 5, 449–451, DOI 10.2307/2589149. MR1699263

[266] Kohji Matsumoto, *A remark on Smith's result on a divisor problem in arithmetic progressions*, Nagoya Math. J. **98** (1985), 37–42, DOI 10.1017/S0027763000021346. MR792769

[267] James Maynard, *Small gaps between primes*, Ann. of Math. (2) **181** (2015), no. 1, 383–413, DOI 10.4007/annals.2015.181.1.7. MR3272929

[268] Paul J. McCarthy, *Introduction to arithmetical functions*, Universitext, Springer-Verlag, New York, 1986, DOI 10.1007/978-1-4613-8620-9. MR815514

[269] Richard J. McIntosh and Eric L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), no. 260, 2087–2094, DOI 10.1090/S0025-5718-07-01955-2. MR2336284

[270] Preda Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195, DOI 10.1515/crll.2004.048. MR2076124

[271] Hugh L. Montgomery, *Primes in arithmetic progressions*, Michigan Math. J. **17** (1970), 33–39. MR257005

[272] Hugh L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, Vol. 227, Springer-Verlag, Berlin-New York, 1971. MR0337847

[273] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007. MR2378655

[274] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics, Vol. 30, Academic Press, London-New York, 1969. MR0249355

[275] J. Morgenbesser, *Gelfond's Sum of Digits Problems*, Doctoral Thesis Vienna University of Technology, 1982

[276] Cristinel Mortici, *A converse of a result about the floor function by Hermite*, Internat. J. Math. Ed. Sci. Tech. **43** (2012), no. 1, 114–118, DOI 10.1080/0020739X.2011.573869. MR2877978

[277] Yoichi Motohashi, *On the distribution of the divisor function in arithmetic progressions*, Acta Arith. **22** (1973), 175–199, DOI 10.4064/aa-22-2-175-199. MR340196

[278] Michael Müger, *On Karamata's proof of the Landau-Ingham Tauberian theorem*, Enseign. Math. **61** (2015), no. 1-2, 45–69, DOI 10.4171/LEM/61-1/2-3. MR3449282

[279] P. J. Murray, *The greatest integer part function*, Master thesis, Oregon State University, 1964

[280] M. Nair, *On Chebyshev-type inequalities for primes*, Amer. Math. Monthly **89** (1982), no. 2, 126–129, DOI 10.2307/2320934. MR643279

[281] Melvyn B. Nathanson, *Additive number theory*, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, 1996. Inverse problems and the geometry of sumsets, DOI 10.1007/978-1-4757-3845-2. MR1477155

[282] Melvyn B. Nathanson, *Affine invariants, relatively prime sets, and a phi function for subsets of* $\{1, 2, \ldots, n\}$, Integers **7** (2007), A1, 7. MR2282182

[283] Melvyn B. Nathanson, *Addictive number theory*, Additive number theory, Springer, New York, 2010, pp. 1–8, DOI 10.1007/978-0-387-68361-4_1. MR2744740

[284] Melvyn B. Nathanson, *Commutative algebra and the linear Diophantine problem of Frobenius*, Integers **18B** (2018), Paper No. A7, 13. MR3794020

[285] Melvyn B. Nathanson and Brooke Orosz, *Asymptotic estimates for phi functions for subsets of* $\{m+1, m+2, \ldots, n\}$, Integers **7** (2007), A54, 5. MR2373116

[286] D. J. Newman, *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly **87** (1980), no. 9, 693–696, DOI 10.2307/2321853. MR602825

[287] D. J. Newman, *Euler's* $\phi$ *function on arithmetic progressions*, Amer. Math. Monthly **104** (1997), no. 3, 256–257, DOI 10.2307/2974791. MR1436048

[288] Hanh My Nguyen and Carl Pomerance, *The reciprocal sum of the amicable numbers*, Math. Comp. **88** (2019), no. 317, 1503–1526, DOI 10.1090/mcom/3362. MR3904154

[289] Harald Niederreiter, *Distribution of Fibonacci numbers* $\bmod 5^k$, Fibonacci Quart. **10** (1972), no. 4, 373–374. MR314751

[290] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers*, 5th ed., John Wiley & Sons, Inc., New York, 1991. MR1083765

[291] Kritkhajohn Onphaeng and Prapanpong Pongsriiam, *Jacobsthal and Jacobsthal-Lucas numbers and sums introduced by Jacobsthal and Tverberg*, J. Integer Seq. **20** (2017), no. 3, Art. 17.3.6, 20. MR3612316

[292] W. Palatsang, P. Pongsriiam, T. Khemaratchatakumthorn, K. Subwattanachai, N. Khuntijit, and N. Kitnak, *Remarks on certain sums involving the floor function*, ScienceAsia, **47**(5) (2021), 640–644.

[293] Wayne Peng, *ABC implies there are infinitely many non-Fibonacci-Wieferich primes*, J. Number Theory **212** (2020), 354–375, DOI 10.1016/j.jnt.2019.11.010. MR4080059

[294] Phakhinkon Phunphayap and Prapanpong Pongsriiam, *Explicit formulas for the $p$-adic valuations of Fibonomial coefficients*, J. Integer Seq. **21** (2018), no. 3, Art. 18.3.1, 33. MR3805746

[295] Phakhinkon Phunphayap and Prapanpong Pongsriiam, *Reciprocal sum of palindromes*, J. Integer Seq. **22** (2019), no. 8, Art. 19.8.6, 13. MR4056413

[296] Phakhinkon Napp Phunphayap, Prapanpong Pongsriiam, and Jeffrey Shallit, *Sumsets associated with Beatty sequences*, Discrete Math. **345** (2022), no. 5, Paper No. 112810, 10, DOI 10.1016/j.disc.2022.112810. MR4369626

[297] István Pink and Márton Szikszai, *A Brocard-Ramanujan-type equation with Lucas and associated Lucas sequences*, Glas. Mat. Ser. III **52(72)** (2017), no. 1, 11–21, DOI 10.3336/gm.52.1.02. MR3662600

[298] Jane Pitman, *Sumsets of finite Beatty sequences*, Electron. J. Combin. **8** (2001), no. 2, Research Paper 15, 23. In honor of Aviezri Fraenkel on the occasion of his 70th birthday. MR1853266

[299] Paul Pollack, *Not always buried deep*, American Mathematical Society, Providence, RI, 2009. A second course in elementary number theory, DOI 10.1090/mbk/068. MR2555430

[300] Paul Pollack, *A generalization of the Hardy-Ramanujan inequality and applications*, J. Number Theory **210** (2020), 171–182, DOI 10.1016/j.jnt.2019.10.004. MR4057524

[301] Paul Pollack, *The maximal size of the $k$-fold divisor function for very large $k$*, J. Ramanujan Math. Soc. **35** (2020), no. 4, 341–345. MR4188678

[302] Richard M. Pollack and Harold N. Shapiro, *The next to last case of a factorial diophantine equation*, Comm. Pure Appl. Math. **26** (1973), 313–325, DOI 10.1002/cpa.3160260303. MR360465

[303] Paul Pollack and Vladimir Shevelev, *On perfect and near-perfect numbers*, J. Number Theory **132** (2012), no. 12, 3037–3046, DOI 10.1016/j.jnt.2012.06.008. MR2965207

[304] D. H. J Polymath, *New equidistribution estimates of Zhang type, and bounded gaps between primes*, preprint available `arXiv:1402.0811v2`.

[305] D. H. J Polymath, *New equidistribution estimates of Zhang type*, preprint available `arXiv:1402.0811v3`.

[306] D. H. J. Polymath, *New equidistribution estimates of Zhang type*, Algebra Number Theory **8** (2014), no. 9, 2067–2199, DOI 10.2140/ant.2014.8.2067. MR3294387

[307] D. H. J. Polymath, *Variants of the Selberg sieve, and bounded intervals containing many primes*, Res. Math. Sci. **1** (2014), Art. 12, 83, DOI 10.1186/s40687-014-0012-7. MR3373710

[308] Carl Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), no. 156, 587–593, DOI 10.2307/2007448. MR628717

[309] Carl Pomerance, *Ruth-Aaron numbers revisited*, Paul Erdős and his mathematics, I (Budapest, 1999), Bolyai Soc. Math. Stud., vol. 11, János Bolyai Math. Soc., Budapest, 2002, pp. 567–579. MR1954715

[310] Carl Pomerance, *Remarks on the Pólya-Vinogradov inequality*, Integers **11** (2011), no. 4, 531–542, DOI 10.1515/integ.2011.039. MR2988079

[311] Carl Pomerance, *The Pólya-Vinogradov Inequality*, Slide presentation in Illinois Number Theory Conference in honor of Harold Diamond 70th Birthday, Available at `https://www.math.dartmouth.edu/~carlp/pvtalk.pdf`

[312] Prapanpong Pongsriiam, *The distribution of the divisor function in arithmetic progressions*, ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–The Pennsylvania State University. MR3067959

[313] Prapanpong Pongsriiam, *A remark on relatively prime sets*, Integers **13** (2013), Paper No. A49, 14. MR3097163

[314] Prapanpong Pongsriiam, *Relatively prime sets, divisor sums, and partial sums*, J. Integer Seq. **16** (2013), no. 9, Article 13.9.1, 11. MR3137930

[315] Prapanpong Pongsriiam, *Local behaviors of the number of relatively prime sets*, Int. J. Number Theory **12** (2016), no. 6, 1575–1593, DOI 10.1142/S1793042116500962. MR3529882

[316] Prapanpong Pongsriiam, *A complete formula for the order of appearance of the powers of Lucas numbers*, Commun. Korean Math. Soc. **31** (2016), no. 3, 447–450, DOI 10.4134/CKMS.c150161. MR3534320

[317] Prapanpong Pongsriiam, *Fibonacci and Lucas numbers which are one away from their products*, Fibonacci Quart. **55** (2017), no. 1, 29–40. MR3620575

[318] Prapanpong Pongsriiam, *Fibonacci and Lucas numbers associated with Brocard-Ramanujan equation*, Commun. Korean Math. Soc. **32** (2017), no. 3, 511–522, DOI 10.4134/CKMS.c160178. MR3682410

[319] Prapanpong Pongsriiam, *Longest arithmetic progressions in reduced residue systems*, J. Number Theory **183** (2018), 309–325, DOI 10.1016/j.jnt.2017.07.017. MR3715239

[320] Prapanpong Pongsriiam, *The order of appearance of factorials in the Fibonacci sequence and certain Diophantine equations*, Period. Math. Hungar. **79** (2019), no. 2, 141–156, DOI 10.1007/s10998-018-0268-6. MR4022197

[321] Prapanpong Pongsriiam, *Fibonacci and Lucas numbers which have exactly three prime factors and some unique properties of $F_{18}$ and $L_{18}$*, Fibonacci Quart. **57** (2019), no. 5, 130–144. MR4034353

[322] Prapanpong Pongsriiam, *Fibonacci and Lucas numbers associated with Brocard-Ramanujan equation II*, Math. Rep. (Bucur.) **22(72)** (2020), no. 3-4, 213–231. MR4233103

[323] Prapanpong Pongsriiam, *Longest arithmetic progressions of palindromes*, J. Number Theory **222** (2021), 362–375, DOI 10.1016/j.jnt.2020.10.018. MR4215820

[324] Prapanpong Pongsriiam, *Combinatorial structure and sumsets associated with Beatty sequences generated by powers of the golden ratio*, Electron. Res. Arch. **30** (2022), no. 7, 2385–2405, DOI 10.3934/era.2022121. MR4420359

[325] Prapanpong Pongsriiam and Kittipong Subwattanachai, *Exact formulas for the number of palindromes up to a given positive integer*, Int. J. Math. Comput. Sci. **14** (2019), no. 1, 27–46. MR3885500

[326] Prapanpong Pongsriiam and Kittipong Subwattanachai, *Arithmetic progressions in the values of a quadratic polynomial*, Amer. Math. Monthly **128** (2021), no. 10, 937–941, DOI 10.1080/00029890.2021.1977884. MR4343355

[327] P. Pongsriiam and R. C. Vaughan, *The divisor function on residue classes I*, Acta Arith. **168**(4) (2015), 369–381.

[328] Prapanpong Pongsriiam and Robert C. Vaughan, *The divisor function on residue classes II*, Acta Arith. **182** (2018), no. 2, 133–181, DOI 10.4064/aa161213-24-10. MR3749366

[329] Prapanpong Pongsriiam and Robert C. Vaughan, *The divisor function on residue classes I*, Acta Arith. **168** (2015), no. 4, 369–382, DOI 10.4064/aa168-4-3. MR3352438

[330] PrimeGrid, Wall–Sun–Sun prime search, `http://www.primegrid.com`

[331] Aayush Rajasekaran, Jeffrey Shallit, and Tim Smith, *Sums of palindromes: an approach via automata*, 35th Symposium on Theoretical Aspects of Computer Science, LIPIcs. Leibniz Int. Proc. Inform., vol. 96, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2018, pp. Art. No. 54, 12. MR3779335

[332] M. Ram Murty, *Problems in analytic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 206, Springer, New York, 2008. Readings in Mathematics. MR2376618

[333] M. Ram Murty, Michael Dewar, and Hester Graves, *Problems in the theory of modular forms*, Institute of Mathematical Sciences Lecture Notes, vol. 1, Hindustan Book Agency, New Delhi, 2015. MR3330491

[334] M. Ram Murty and Jody Esmonde, *Problems in algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 190, Springer-Verlag, New York, 2005. MR2090972

[335] M. Ram Murty and Akshaa Vatwani, *A higher rank Selberg sieve with an additive twist and applications*, Funct. Approx. Comment. Math. **57** (2017), no. 2, 151–184, DOI 10.7169/facm/1622. MR3732894

[336] Srinivasa Ramanujan, *Highly composite numbers*, Proc. London Math. Soc. (2) **14** (1915), 347–409.

[337] Srinivasa Ramanujan, *A proof of Bertrand's postulate*, J. Indian Math. Soc. **11** (1919), 181–182.

[338] Srinivasa Ramanujan, *The lost notebook and other unpublished papers*, Springer-Verlag, Berlin; Narosa Publishing House, New Delhi, 1988. With an introduction by George E. Andrews. MR947735

[339] Srinivasa Ramanujan, *Collected Papers*, Cambridge University Press, Cambridge, 1927; reprinted by Chelsea, New York, 1962; reprinted by the American Mathematical Society, Providence, RI, 2000

[340] Srinivasa Ramanujan, *Notebooks. Vols. 1, 2*, Tata Institute of Fundamental Research, Bombay, 1957. MR0099904

[341] Xiao-Zhi Ren and Yong-Gao Chen, *On near-perfect numbers with two distinct prime factors*, Bull. Aust. Math. Soc. **88** (2013), no. 3, 520–524, DOI 10.1017/S0004972713000178. MR3189304

[342] Paulo Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996, DOI 10.1007/978-1-4612-0759-7. MR1377060

[343] David Ross Richman, *A sum involving the greatest-integer function*, Integers **19** (2019), Paper No. A42, 16. MR3997447

[344] Florian K. Richter, *A new elementary proof of the Prime Number Theorem*, Bull. Lond. Math. Soc. **53** (2021), no. 5, 1365–1375, DOI 10.1112/blms.12503. MR4332834

[345] G. J. Rieger, *Aufeinanderfolgende Zahlen als Summen von zwei Quadraten* (German), Nederl. Akad. Wetensch. Proc. Ser. A 68 = Indag. Math. **27** (1965), 208–220. MR0175871

[346] A. M. Robles-Pérez and J. C. Rosales, *The Frobenius number for sequences of triangular and tetrahedral numbers*, J. Number Theory **186** (2018), 473–492, DOI 10.1016/j.jnt.2017.10.014. MR3758226

[347] P. Roggero, M. Nardelli, and F. Di Noto, *Sum of the reciprocals of famous series: mathematical connections with some sectors of theoretical physics and string theory*, preprint, 2016. Available at `http://empslocal.ex.ac.uk/people/staff/mrwatkin/zeta/nardelli2017a.pdf`

[348] K. H. Rosen, *Elementary Number Theory*, Addison Wesley, International Fifth Edition, 2005

[349] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR137689

[350] Pongpol Ruankong and Kantaphon Kuhapatanakul, *Approximating sums of consecutive integral roots*, J. Integer Seq. **22** (2019), no. 6, Art. 19.6.8, 8. MR4020276

[351] Manasi Kumari Sahukar and G. K. Panda, *Arithmetic functions of balancing numbers*, Fibonacci Quart. **56** (2018), no. 3, 246–251, DOI 10.2514/1.j056001. MR3849220

[352] Manasi Kumari Sahukar and Gopal Krishna Panda, *Diophantine equations with balancing-like sequences associated to Brocard-Ramanujan-type problem*, Glas. Mat. Ser. III **54(74)** (2019), no. 2, 255–270, DOI 10.3336/gm.54.2.01. MR4043130

[353] Peter W. Saltzman and Pingzhi Yuan, *On sums of consecutive integral roots*, Amer. Math. Monthly **115** (2008), no. 3, 254–261, DOI 10.1080/00029890.2008.11920524. MR2395037

[354] József Sándor, Dragoslav S. Mitrinović, and Borislav Crstici, *Handbook of number theory. I*, Springer, Dordrecht, 2006. Second printing of the 1996 original. MR2186914

[355] Lowell Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II*, Math. Comp. **30** (1976), no. 134, 337–360, DOI 10.2307/2005976. MR457374

[356] Wolfgang Schwarz and Jürgen Spilker, *Arithmetical functions*, London Mathematical Society Lecture Note Series, vol. 184, Cambridge University Press, Cambridge, 1994. An introduction to elementary and analytic properties of arithmetic functions and to some of their almost-periodic properties, DOI 10.1017/CBO9781107359963.014. MR1274248

[357] S. L. Segal, *A note on normal order and the Euler $\phi$-function*, J. London Math. Soc. **39** (1964), 400–404, DOI 10.1112/jlms/s1-39.1.400. MR188168

[358] Atle Selberg, *An elementary proof of the prime-number theorem*, Ann. of Math. (2) **50** (1949), 305–313, DOI 10.2307/1969455. MR29410

[359] Atle Selberg, *On the zeros of Riemann's zeta-function on the critical line*, Arch. Math. Naturvid. **45** (1942), no. 9, 101–114. MR12625

[360] Atle Selberg, *On the zeros of Riemann's zeta-function*, Skr. Norske Vid.-Akad. Oslo I **1942** (1942), no. 10, 59. MR10712

[361] J. Shallit, *Problem B–441*, Fibonacci Quart. **18** (1980), 370.

[362] J. Shallit and H. Klauser, *Sum of base–$b$ palindrome reciprocals*, Fibonacci Quart. **19** (1981), 469.

[363] Harold N. Shapiro, *On primes in arithmetic progression. II*, Ann. of Math. (2) **52** (1950), 231–243, DOI 10.2307/1969521. MR36262

[364] Harold N. Shapiro, *Introduction to the theory of numbers*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1983. MR693458

[365] Wai Chee Shiu and Chuan I Chu, *Distribution of the Fibonacci numbers modulo* $3^k$, Fibonacci Quart. **43** (2005), no. 1, 22–28. MR2129116

[366] Temba Shonhiwa, *On relatively prime sets counting functions*, Integers **10** (2010), A39, 465–476, DOI 10.1515/INTEG.2010.039. MR2798617

[367] W. Sierpiński, *Remarque sur la répartition des nombres premiers* (French), Colloq. Math. **1** (1948), 193–194, DOI 10.4064/cm-1-3-193-194. MR28332

[368] W. Sierpiński, *Sur les nombres pseudoparfaits* (French), Mat. Vesnik **2(17)** (1965), 212–213. MR199147

[369] W. Sierpiński, *250 problems in elementary number theory*, Modern Analytic and Computational Methods in Science and Mathematics, No. 26, American Elsevier Publishing Co., Inc., New York; PWN—Polish Scientific Publishers, Warsaw, 1970. MR0269580

[370] W. Sierpiński, *Elementary theory of numbers*, 2nd ed., North-Holland Mathematical Library, vol. 31, North-Holland Publishing Co., Amsterdam; PWN—Polish Scientific Publishers, Warsaw, 1988. Edited and with a preface by Andrzej Schinzel. MR930670

[371] Joseph H. Silverman, *Wieferich's criterion and the* $abc$*-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237, DOI 10.1016/0022-314X(88)90019-4. MR961918

[372] Jamie Simpson, *Intersecting rational Beatty sequences*, Integers **13** (2013), Paper No. A50, 13. MR3097164

[373] R. Sivaramakrishnan, *Classical theory of arithmetic functions*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 126, Marcel Dekker, Inc., New York, 1989. MR980259

[374] N. J. A. Sloane, *On-Line Encyclopedia of Integer Sequences*, `http://oeis.org`

[375] David Eugene Smith, *A source book in mathematics*, Dover Publications, Inc., New York, 1959. 2 vols. MR0106139

[376] Robert A. Smith, *The generalized divisor problem over arithmetic progressions*, Math. Ann. **260** (1982), no. 2, 255–268, DOI 10.1007/BF01457239. MR664379

[377] Lawrence Somer and Michal Křížek, *Fixed points and upper bounds for the rank of appearance in Lucas sequences*, Fibonacci Quart. **51** (2013), no. 4, 291–306. MR3131009

[378] Lawrence Somer and Michal Křížek, *Identically distributed second-order linear recurrences modulo* $p$, Fibonacci Quart. **53** (2015), no. 4, 290–312. MR3423902

[379] Lawrence Somer and Michal Křížek, *Nondefective integers with respect to certain Lucas sequences of the second kind*, Integers **18** (2018), Paper No. A35, 13. MR3794025

[380] Gökhan Soydan, László Németh, and László Szalay, *On the Diophantine equation* $\sum_{j=1}^{k} jF_j^p = F_n^q$, Arch. Math. (Brno) **54** (2018), no. 3, 177–188, DOI 10.5817/AM2018-3-177. MR3847324

[381] Richard P. Stanley, *Enumerative combinatorics. Volume 1*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012. MR2868112

[382] Richard P. Stanley, *Enumerative combinatorics. Vol. 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin, DOI 10.1017/CBO9780511609589. MR1676282

[383] Elias M. Stein and Rami Shakarchi, *Complex analysis*, Princeton Lectures in Analysis, vol. 2, Princeton University Press, Princeton, NJ, 2003. MR1976398

[384] Cameron L. Stewart, *On divisors of Lucas and Lehmer numbers*, Acta Math. **211** (2013), no. 2, 291–314, DOI 10.1007/s11511-013-0105-y. MR3143892

[385] Jörn Steuding and Pascal Stumpf, *On the Frobenius problem for Beatty sequences*, Indag. Math. (N.S.) **28** (2017), no. 1, 132–137, DOI 10.1016/j.indag.2016.11.020. MR3597039

[386] John Stillwell, *Elements of number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003, DOI 10.1007/978-0-387-21735-2. MR1944957

[387] Pascal Stumpf, *A short note on reduced residues*, Integers **17** (2017), Paper No. A4, 4, DOI 10.1002/pamm.201710316. MR3619681

[388] Zhi-Wei Sun, *Refining Lagrange's four-square theorem*, J. Number Theory **175** (2017), 167–190, DOI 10.1016/j.jnt.2016.11.008. MR3608186

[389] Zhi-Wei Sun's homepage `math.nju.edu.cn/~zwsun/`

[390] C. F. Sun and Z. C. He, *On odd deficient-perfect numbers with four distinct prime divisors*, (2019) `arXiv:1908.04932`.

[391] Zhi Hong Sun and Zhi Wei Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), no. 4, 371–388, DOI 10.4064/aa-60-4-371-388. MR1159353

[392] László Szalay, *Diophantine equations with binary recurrences associated to the Brocard-Ramanujan problem*, Port. Math. **69** (2012), no. 3, 213–220, DOI 10.4171/PM/1914. MR2988159

[393] E. Szemerédi, *On sets of integers containing no $k$ elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245, DOI 10.4064/aa-27-1-199-245. MR369312

[394] S. Tadee and V. Laohakosol, *Complementary sets and Beatty functions*, Thai J. Math. **3** (2005), no. 1, 27–33, DOI 10.1155/2005/165785. MR2306299

[395] Min Tang, *Relatively prime sets and a phi function for subsets of* $\{1, 2, \ldots, n\}$, J. Integer Seq. **13** (2010), no. 7, Article 10.7.6, 5. MR2669387

[396] T. Tao, *A Comment on MathOverflow* (*2015*), available online at `https://mathoverflow.net/questions/206151/is-there-an-arbitrarily-long-arithmetic-progression-whose-members-are-palindrome`

[397] Terence Tao and Van H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2010. Paperback edition [of MR2289012]. MR2573797

[398] Terence Tao and Tamar Ziegler, *The primes contain arbitrarily long polynomial progressions*, Acta Math. **201** (2008), no. 2, 213–305, DOI 10.1007/s11511-008-0032-5. MR2461509

[399] Terence Tao and Tamar Ziegler, *Erratum to "The primes contain arbitrarily long polynomial progressions"* [*MR2461509*], Acta Math. **210** (2013), no. 2, 403–404, DOI 10.1007/s11511-013-0097-7. MR3070570

[400] Terence Tao and Tamar Ziegler, *Polynomial patterns in the primes*, Forum Math. Pi **6** (2018), e1, 60, DOI 10.1017/fmp.2017.3. MR3778204

[401] Min Tang and Min Feng, *On deficient-perfect numbers*, Bull. Aust. Math. Soc. **90** (2014), no. 2, 186–194, DOI 10.1017/S0004972714000082. MR3251999

[402] Min Tang, Xiaoyan Ma, and Min Feng, *On near-perfect numbers*, Colloq. Math. **144** (2016), no. 2, 157–188, DOI 10.4064/cm7678-10-2018. MR3493818

[403] Min Tang, Xiao-Zhi Ren, and Meng Li, *On near-perfect and deficient-perfect numbers*, Colloq. Math. **133** (2013), no. 2, 221–226, DOI 10.4064/cm133-2-8. MR3145514

[404] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572, DOI 10.2307/2118560. MR1333036

[405] M. Technau, *On Beatty sets and some generalisations thereof*, Ph.D. dissertation, Würzburg University Press, 2018.

[406] M. Technau, *Generalized Beatty sets*, Notes on Number Theory and Discrete Mathematics, **25** (2019), 127–135.

[407] Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas. MR1342300

[408] Szabolcs Tengely, *On the Lucas sequence equation* $\frac{1}{U_n} = \sum_{k=1}^{\infty} \frac{U_{k-1}}{x^k}$, Period. Math. Hungar. **71** (2015), no. 2, 236–242, DOI 10.1007/s10998-015-0101-4. MR3421697

[409] Thotsaporn Thanatipanonda and Elaine Wong, *Curious bounds for floor function sums*, J. Integer Seq. **21** (2018), no. 1, Art. 18.1.8, 19. MR3771676

[410] R. Tijdeman, *Fraenkel's conjecture for six sequences*, Discrete Math. **222** (2000), no. 1-3, 223–234, DOI 10.1016/S0012-365X(99)00411-2. MR1771401

[411] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, 2nd ed., The Clarendon Press, Oxford University Press, New York, 1986. Edited and with a preface by D. R. Heath-Brown. MR882550

[412] László Tóth, *On the number of certain relatively prime subsets of* $\{1, 2, \ldots, n\}$, Integers **10** (2010), A35, 407–421, DOI 10.1515/INTEG.2010.035. MR2684131

[413] Amitabha Tripathi, *On a special case of the Frobenius problem*, J. Integer Seq. **20** (2017), no. 7, Art. 17.7.2, 12. MR3687763

[414] Amitabha Tripathi, *Formulae for the Frobenius number in three variables*, J. Number Theory **170** (2017), 368–389, DOI 10.1016/j.jnt.2016.05.027. MR3541713

[415] Paul Turán, *On a Theorem of Hardy and Ramanujan*, J. London Math. Soc. **9** (1934), no. 4, 274–276, DOI 10.1112/jlms/s1-9.4.274. MR1574877

[416] Helge Tverberg, *On some number-theoretic sums introduced by Jacobsthal*, Acta Arith. **155** (2012), no. 4, 349–351, DOI 10.4064/aa155-4-1. MR2997574

[417] J. V. Uspensky, *On a Problem Arising Out of the Theory of a Certain Game*, Amer. Math. Monthly **34** (1927), no. 10, 516–521, DOI 10.2307/2299838. MR1521314

[418] S. Vajda, *Fibonacci & Lucas numbers, and the golden section*, Ellis Horwood Series: Mathematics and its Applications, Ellis Horwood Ltd., Chichester; Halsted Press [John Wiley & Sons, Inc.], New York, 1989. Theory and applications; With chapter XII by B. W. Conolly. MR1015938

[419] A. van der Poorten, *Fermat's four squares theorem*, preprint available at `arXiv:0712.3850`.

[420] Akshaa Vatwani, *A higher rank Selberg sieve and applications*, Czechoslovak Math. J. **68(143)** (2018), no. 1, 169–193, DOI 10.21136/CMJ.2017.0410-16. MR3783592

[421] R. C. Vaughan, *Mean value theorems in prime number theory*, J. London Math Soc. (2) **10** (1975), 153–162, DOI 10.1112/jlms/s2-10.2.153. MR0376567

[422] R. C. Vaughan, *The Hardy-Littlewood method*, 2nd ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, Cambridge, 1997, DOI 10.1017/CBO9780511470929. MR1435742

[423] R. C. Vaughan, *On a variance associated with the distribution of general sequences in arithmetic progressions. I*, R. Soc. Lond. Philos. Trans. Ser. A Math. Phys. Eng. Sci. **356** (1998), no. 1738, 781–791, DOI 10.1098/rsta.1998.0185. MR1620836

[424] R. C. Vaughan, *On a variance associated with the distribution of general sequences in arithmetic progressions. II*, R. Soc. Lond. Philos. Trans. Ser. A Math. Phys. Eng. Sci. **356** (1998), no. 1738, 793–809, DOI 10.1098/rsta.1998.0185.

[425] R. C. Vaughan, *The general Goldbach problem with Beatty primes*, Ramanujan J. **34** (2014), no. 3, 347–359, DOI 10.1007/s11139-013-9501-3. MR3231316

[426] R. C. Vaughan and T. D. Wooley, *Waring's problem: a survey*, Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 301–340, DOI 10.1198/004017002320256684. MR1956283

[427] A. I. Vinogradov, *Correction to the paper of A. I. Vinogradov "On the density hypothesis for the Dirichlet L-series"* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **30** (1966), 719–720. MR0194397

[428] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, C. R. Acad. Sci. URSS **15** (1937), 6–7.

[429] Nicolai N. Vorobiev, *Fibonacci numbers*, Birkhäuser Verlag, Basel, 2002. Translated from the 6th (1992) Russian edition by Mircea Martin, DOI 10.1007/978-3-0348-8107-4. MR1954396

[430] Georges Voronoi, *Sur un problème du calcul des fonctions asymptotiques* (French), J. Reine Angew. Math. **126** (1903), 241–282, DOI 10.1515/crll.1903.126.241. MR1580627

[431] Arnold Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie* (German), Mathematische Forschungsberichte, XV, VEB Deutscher Verlag der Wissenschaften, Berlin, 1963. MR0220685

[432] D. D. Wall, *Fibonacci series modulo* $m$, Amer. Math. Monthly **67** (1960), 525–532, DOI 10.2307/2309169. MR120188

[433] Z. Wang, *A City of Nice Mathematics* (in Chinese), The Democracy and Construction Press, Beijing. 2000

[434] Norbert Wiener, *Tauberian theorems*, Ann. of Math. (2) **33** (1932), no. 1, 1–100, DOI 10.2307/1968102. MR1503035

[435] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, DOI 10.2307/2118559. MR1333035

[436] Aurel Wintner, *The Theory of Measure in Arithmetical Semi-Groups*, publisher unknown, Baltimore, Md., 1944. MR0015083

[437] Wolfram Mathworld, *Dirichlet divisor problem*, available at `http://mathworld.wolfram.com/DirichletDivisorProblem.html`

[438] Hai-Liang Wu and Zhi-Wei Sun, *On the 1-3-5 conjecture and related topics*, Acta Arith. **193** (2020), no. 3, 253–268, DOI 10.4064/aa180911-9-8. MR4071805

[439] W. A. Wythoff, *A modification of the game of nim*, Nieuw Arch. Wiskd. **2** (1905–07), 199–202.

[440] D. Zagier, *Newman's short proof of the prime number theorem*, Amer. Math. Monthly **104** (1997), no. 8, 705–708, DOI 10.2307/2975232. MR1476753

[441] X. Zhan, *Formulae for sums of consecutive square roots*, Math. Intelligencer **27**(4) (2005), 4–5.

[442] Yitang Zhang, *Bounded gaps between primes*, Ann. of Math. (2) **179** (2014), no. 3, 1121–1174, DOI 10.4007/annals.2014.179.3.7. MR3171761

# Subject Index

abc-conjecture, 58
Abel summation formula, 110
Abel's test, 109
abscissa of absolute convergence, 231
abscissa of convergence, 231
additive basis, 314
additively avoidable, 223
analytic continuation, 247, 253
arithmetic progression, 187, 208, 214, 218, 219, 225, 258
asymptotic, 101, 131, 163, 170
asymptotic additive basis, 314

Beatty sequence, 97
  homogeneous, 97
  inhomogeneous, 97
Bernoulli number, 117, 251
Bernoulli polynomial, 117, 251
Bertrand's postulate, 178
big *O*, 100
Birch's theorem, 162
Bombieri-Vinogradov theorem, 287
Brun's sieve, 295

canonical factorization, 7
Cauchy criterion, 239
Cauchy-Schwarz inequality, 303
ceiling function, least integer function, 65
character
  Dirichlet, 194, 222
  prinicipal, 188
Chebyshev's $\psi$-function, 170
Chebyshev's $\theta$-function, 170
Chinese remainder theorem, 13, 192
circle method, 329
composite, 6, 25
congruence, 10, 17
critical line, 254
critical strip, 254

Diophantine equation, 4, 17, 60, 211, 224, 227
Dirichlet
  character, 188, 194, 222, 230
  divisor problem, 164
  hyperbola method, 137
  inverse, 40

  *L*-function, 188, 198
  *L*-series, 198, 230
  product, convolution, multiplication, 38, 245
  series, 230, 245
  theorem on primes in arithmetic progressions, 187, 203, 214, 221, 285
distribution function, 163
divisibility, 1
division algorithm, 2
divisor functions, 34, 38, 54, 129, 131, 133, 139, 141, 143, 161, 166, 219
divisor sum, 42

Elliott-Halberstam conjecture, 287, 291
Eratosthenes' sieve, 294
Euclidean algorithm, 3
Euler
  constant, 115, 124, 130, 178, 181, 229
  criterion, 23
  function, 12, 34, 44, 55, 134, 147, 161, 195, 219–221
  product formula, 165, 242
  summation formula, 114, 175
  theorem, 17
Euler-Maclaurin summation formula, 117

factorial, 125, 211, 218
Fermat
  last theorem, 57
  little theorem, 17
  number, 29
Fibonacci
  Association, 29
  number, 29, 222, 225
  *Quarterly*, 29
  sequence, 25, 57, 220
Fibonacci-Wieferich prime, 57
Fibonomial coefficients, 94
floor function, greatest integer function, 65, 79, 166
fractional part, 65, 166
Frobenius numbers, 29
function
  additive, 36
  analytic, 230
  arithmetic, 33, 129
  completely additive, 36, 52
  completely multiplicative, 36, 48
  differentiable, 230
  entire, 230
  holomorphic, 230
  monotone, 104, 130
  multiplicative, 36, 48, 53, 146, 167, 243
  strongly additive, 36, 52
  strongly multiplicative, 36
  unimodal, 104
functional equation, 254
fundamental theorem of arithmetic, 7, 243

Gauss
  circle problem, 165
  generalization of Wilson's theorem, 19
  lemma, 24
geometric progression, 210
Goldbach's conjecture, 27
Great Internet Mersenne Prime Search (GIMPS), 27

greatest common divisor, 2, 5
group, 57, 187
  character, 188
  direct product, 190
  direct sum, 190
  dual, 189

half-plane of convergence, 231
Hensel's lemma, 19
Hermite's identity, 71

integer part, 65
Iverson notation, 94

Lagrange's theorem, 17
Laurent series, 229
least common multiple, 6
Legendre symbol, 23
lifting the exponent lemma, 20, 213
limit infimum, 142
limit supremum, 142
Liouville's function, 34, 44, 57
little *o*, 101
logarithmic integral, 170, 184
Lucas sequence, 29, 223

Möbius
  function, 34, 38, 53, 163, 219
  inversion formula, 43, 49
major arcs, 332
Mann's Theorem, 324
mean value, 130
Mersenne prime, 27
Mertens' theorems, 178
minor arcs, 332

nontrivial zeros, 254

order
  average, 130, 131, 161
  extremal, 131, 141, 161
  maximal, 130, 143, 161
  minimal, 130, 145, 162
  normal, 130, 150, 161
  of *a* modulo *m*, 22
order (or the rank) of appearance, 56
orthogonality relation, 192

*p*-adic valuation, *p*-adic order, 9, 20, 94, 124, 211
partial summation, 108
perfect number, 27
Perron's formula, 267
prime, 6, 25, 130, 144, 169, 178, 184, 187, 214, 218, 219, 257, 259, 263, 285, 288, 290
primitive root, 19, 23
primitive set, 32
Pythagorean triple, 226

quadratic nonresidue, 23
quadratic reciprocity law, 24, 79
quadratic residue, 23
quotient, 2

Ramanujan's sum, 289
relatively prime, coprime, 2, 32, 187, 258
remainder, 2, 74, 76
residue system, 12, 74, 192, 194, 225
Riemann
  hypothesis, 164, 222, 253, 269, 287
  integral, 99, 112
  zeta function, 167, 229, 266

Riemann-Stieltjes integral, 112
Ruth-Aaron number, 63

saw–tooth function, 75
Schnirelmann density, 321
Schnirelmann's basis theorem,
    321
Siegel-Walfisz theorem, 286
square, 24, 26, 30, 31, 209, 219,
    221, 223, 284
Stirling formula, 125
sum of digits, 26, 31
sumset, 314

Turán-Kubilius inequality, 154

Vinogradov notation, 100
von Mangoldt's function, 35,
    161, 170, 283

Wall-Sun-Sun prime, 57
Waring's problem, 316, 317
Wieferich prime, 58
Wiener-Ikehara theorem, 259
Wilson's theorem, 17
Wolstenholme's theorem, 19
Wythoff sequence, 98

zero free region, 249, 253, 268

# Name Index

Aldaz, 221
Alladi, 63, 223
Alladi-Erdös, 56, 63
Anderson, 62
Andreescu, 17, 80
Andrews, 126
Andrica, 17, 80
Angelo, 32
Apostol, 1, 13, 17, 113, 184, 187, 221
Aursukaree, 72
Axer, 167
Axler, 185, 278

Bachmann, 123
Baczkowski, 126
Bambah, 31
Banks, 228, 290
Barat, 98
Barban, 288
Bateman, 259
Bayless, 30, 279
Beatty, 98
Belbachir, 29
Berndt, 126, 165
Besicovitch, 32
Bhargava, 19
Bicknell–Johnson, 223
Birch, 162
Blomer, 290
Bombieri, 286
Bourgain, 164, 165
Brocard, 228
Brown, 222
Bruckman, 62
Bugeaud, 127
Bundschuh, 227
Burnside, 125
Burr, 227

Cameron, 32
Cantor, 221
Carlitz, 96
Carmichael, 56, 57
Catalan, 223
Cauchy, 233, 313
Chebyshev, 173, 258
Chen, 27, 28, 165, 223
Chow, 223
Chowla, 31
Chu, 227
Chudakov, 254
Cira, 56
Cochrane, 31
Cohen, 28
Cojocaru, 280, 293
Conlon, 215
Conrey, 255, 256
Cosgrave, 19
Cubre, 62
Cucurezeanu, 17

Dancs, 289
Davenport, 222, 287, 288, 329, 333
De Koninck, 275

de la Vallée Poussin, 167, 169, 254, 258
Delange, 167
Dewar, 280
Di Noto, 30
Diamond, 259
Dickson, 221
Dilcher, 19
Dirichlet, 65, 258
Domotorp, 227
Dorais, 57, 60
Dressler, 31
Duncan, 280
Dunn, 222
Dusart, 185, 278

Eisenstein, 79, 94
Elliot, 150, 154
Erdös, 29, 32, 57, 63, 126, 150, 223, 227, 266
Esmonde, 280
Euclid, 7, 257
Euler, 27, 124, 229, 257

Faber, 185
Feng, 28, 255
Fermat, 221
Filaseta, 126
Finch, 124
Fox, 215
Fraenkel, 98
Freiman, 314
Friedlander, 289, 293
Gallagher, 287, 288
Gauss, 65, 79, 86, 94, 169, 173, 184, 257
Gelfond, 31, 187
Goldbach, 290
Goldfeld, 259, 267
Goldston, 289, 291
Graham, 68, 94, 98, 126
Granville, 224
Graves, 280
Green, 215, 224
Greene, 237
Grimson, 96
Guersenzvaig, 89
Guy, 225, 280

Hacks, 85
Hadamard, 169, 258
Haertel, 65
Halberstam, 288, 293, 314
Hammer, 95
Hanson, 184
Hardy, 1, 13, 19, 124, 150, 164, 165, 225, 230, 254, 266, 275
Harman, 228
Harminc, 227
Harrington, 222
Hassani, 127
He, 28
Heath-Brown, 290
Helfgott, 27
Hildebrand, 98, 279
Hirschhorn, 126
Hoggatt, 223
Hooley, 31, 288
Hua, 27, 254, 293
Huxley, 287

Indlekofer, 31
Ingham, 124, 254, 269
Iverson, 65
Ivić, 126, 230, 256
Iwaniec, 165, 293

Jacobson, 227
Jacobsthal, 96
Jaidee, 127
Jarden, 221
Jones, 222

Křižek, 60, 227
Kac, 150
Kadiri, 185
Kawsumarng, 94
Khaochim, 60
Khelladi, 29
Kim, 126, 165
Kimberling, 98
Kinlaw, 30, 279
Klaška, 58, 60
Klyve, 30, 57, 60, 279
Knuth, 68, 94
Kobayashi, 30
Kolesnik, 165
Korevaar, 259
Korobov, 254

Koshy, 29
Kra, 215
Krandel, 223
Krantz, 237
Kronecker, 65
Kuhapatanakul, 95
Kuipers, 227

Lagarias, 62
Landau, 30, 86, 123, 164, 165, 254, 279
Laohakosol, 98
Legendre, 65, 169, 257
Levinson, 255
Li, 28, 98
Lichtman, 30, 32
Lichtmann, 32
Linnik, 187
Littlewood, 124, 225, 254
Liu, 126
Long, 223
Luca, 61, 126, 275

Ma, 28
Mackenzie, 290
Makowski, 223
Marques, 59, 60, 228
Martin, 221
Maynard, 291
McCarthy, 56
McEliece, 68
Mcintosh, 57
Merten, 277
Mignotte, 127
Mihăilescu, 224
Montgomery, 1, 17, 19, 113, 167, 181, 187, 222, 230, 254, 258, 267, 279, 280, 287, 288, 293
Mordell, 221
Morgenbesser, 31
Mortici, 93
Motohashi, 290
Mozzochi, 165
Murray, 65, 84
Murty, 293

Nardelli, 30
Nathanson, 32, 293, 314
Newman, 220, 221, 259
Nguyen, 30
Niederreiter, 227
Niven, 1, 17, 19

Obláth, 227
On-Line Encyclopedia of Integer Sequences (OEIS), 27, 30, 32, 57, 64, 125, 224
Onphaeng, 68, 96
Orr, 280

Pólya, 221
Pólya–Vinogradov, 222
Panda, 127, 228
Patashnik, 68, 94
Peng, 58
Perichon, 224
Phillips, 222
Phunphayap, 30, 94
Pink, 228
Pintz, 291
Pitman, 98
Polignac, 290
Pollack, 28, 187, 211, 221, 228, 279, 293
Polymath, 291
Pomerance, 30, 32, 57, 61, 63, 126, 222
Pongsriiam, 30, 32, 59, 60, 68, 94, 96, 98, 126, 165, 222, 225, 227, 288, 290
Poorten, 222
PrimeGrid project, 224

Ram Murty, 280
Ramanujan, 125, 150, 173, 184, 228, 275
Ramaré, 185, 278
Recamán, 225
Ren, 28
Reynolds, 224

Ribenboim, 57, 221
Richert, 254, 293
Richman, 95
Rieger, 30
Riemann, 258
Riesz, 230
Robin, 185
Roettger, 57
Rogers, 280
Roggero, 30
Rosen, 1, 16
Rosser, 184, 185, 278
Roth, 293, 314
Rouse, 62
Ruankong, 95

Sahukar, 127, 228
Saltzman, 95
Schinzel, 221
Schoenfeld, 184, 185, 278
Segal, 162
Selberg, 31, 255, 258, 264, 266
Shakarchi, 237
Shapiro, 187, 228
Shevelev, 28
Shiu, 227
Shiue, 227
Shparlinski, 126, 228, 290
Sierpiński, 28, 221, 222
Siksek, 127
Simpson, 98
Sivaramakrishnan, 56
Smarandache, 56
Somer, 60, 227
Soták, 227
Soydan, 228
Spivey, 89
Stein, 237
Stewart, 60
Stillwell, 17
Stumpf, 225
Subwattanachai, 94, 222
Sun, 28, 31, 57, 60
Sylvester, 65
Szalay, 228
Szemerédi, 224
Szikszai, 228

Tadee, 98
Tang, 28
Tao, 215, 224, 227, 291, 314
Tatuzawa, 254
Technau, 98, 228
Tenenbaum, 150, 254, 279
Thanatipanonda, 96
Tijdeman, 98
Titchmarsh, 230, 254, 256, 269
Trifonov, 126
Trojovský, 60
Turán, 130, 150
Tverberg, 96

Uspensky, 98

Vajda, 29
van der Corput, 165
Varju, 98
Vaughan, 27, 113, 126, 165, 167, 181, 184, 187, 221, 222, 228, 230, 254, 258, 267, 279, 280, 287, 288, 290, 293, 314, 329, 333
Villarino, 126
Vinogradov, 27, 100, 124, 165, 254, 286, 287
Vorobiev, 9
Voronoï, 164–166
Vu, 314

Walfisz, 163
Wall, 57, 60
Wang, 95
Watt, 164, 165
Wiles, 57
Wintner, 167
Wong, 96
Wooley, 293, 333
Wright, 1, 13, 19
Wroblewski, 224
Wu, 31
Wythoff, 98

Xie, 98

Yildirim, 291
Young, 127, 255
Yuan, 95

Zagier, 259

Zaharescu, 126, 165
Zhan, 95
Zhang, 126, 288, 291
Zhao, 215
Ziegler, 224
Zuckerman, 1, 17, 19

*Continued from unnumbered page iv*

**Library of Congress Cataloging-in-Publication Data**

Names: Pongsriiam, Prapanpong, 1980– author.
Title: Analytic number theory for beginners / Prapanpong Pongsriiam. Other titles: Introduction to analytic number theory
Description: Second edition. | Providence, Rhode Island : American Mathematical Society, [2023] | Series: Student mathematical library, 1520-9121 ; volume 103 | Revised edition of: Introduction to analytic number theory / Prapanpong Pongsriiam. First edition. 2020. | Includes bibliographical references and index.
Identifiers: LCCN 2023001240 | (paperback) ISBN 9781470464448 | (ebook) ISBN 9781470473570
Subjects: LCSH: Number theory–Textbooks. | AMS: Number theory – Instructional exposition (textbooks, tutorial papers, etc.). | Number theory – Research exposition (monographs, survey articles). | Number theory – Elementary number theory. | Number theory – Sequences and sets. | Number theory – Multiplicative number theory. | Number theory – Additive number theory; partitions.
Classification: LCC QA241 .P663 2023 | DDC 512.7/3–dc23/eng20230429
LC record available at https://lccn.loc.gov/2023001240

This new edition of *Analytic Number Theory for Beginners* presents a friendly introduction to analytic number theory for both advanced undergraduate and beginning graduate students, and offers a comfortable transition between the two levels. The text starts with a review of elementary number theory and continues on to present less commonly covered topics such as multiplicative functions, the floor function, the use of big $O$, little $o$, and Vinogradov notation, as well as summation formulas. Standard advanced topics follow, such as the Dirichlet $L$-function, Dirichlet's Theorem for primes in arithmetic progressions, the Riemann Zeta function, the Prime Number Theorem, and, new in this second edition, sieve methods and additive number theory.

The book is self-contained and easy to follow. Each chapter provides examples and exercises of varying difficulty and ends with a section of notes which include a chapter summary, open questions, historical background, and resources for further study. Since many topics in this book are not typically covered at such an accessible level, *Analytic Number Theory for Beginners* is likely to fill an important niche in today's selection of titles in this field.

ISBN 978-1-4704-6444-8

9 781470 464448

**STML/103**

For additional information
and updates on this book, visit
**www.ams.org/bookpages/stml-103**

AMS
www.ams.org